平成13年度 社会安全研究財団委託調査研究報告書

不正アクセス禁止法の円滑な施行の為の情報収集

平成14年3月

（2002年）

コンピュータセキュリティ対策委員会

代表 清瀬 紀次

はじめに

ここ近年で、世界的にインターネットが普及した結果、日本を含め諸外国の人々にとってインターネットは重要なメディアとして利用されている。電子メールは物理的な距離を越えて短時間の内に相手に届くことが可能であり、日本では特に携帯電話で送受信ができるため広く利用されている。また、Web サイトを利用した電子商取引も活発に行われている。多くの企業がWeb サイトを用意し様々なサービスを展開しており、Web サイトで書籍を購入したり、チケットの予約をしたりと利用者の便宜を図っている。そして、インターネットは多くの人々の生活に入り込み、「なくてはならない存在」となってきている。

ただしこれらの正の側面と同時に、その負の側面の存在を見逃すことはできない。コンピュータ・システムに直接被害を与える不正アクセス行為の増加は増加し、そのメディアとしての利便性からインターネットを利用した詐欺、悪質商法などの犯罪や、SPAM メールといった問題も多く発生している。また、インターネットには国境がないため、簡単に世界中の情報にアクセスすることができる反面、犯罪も国境を越えて容易に行われることになる。それらの犯罪を取り締まるには、インターネットに接続している各国で取り締まるための国内法規を制定すると同時に、諸国がお互いに協力していく国際体制が必要になる。

日本においては、2001 年 2 月 13 日から「不正アクセス行為の禁止等に関する法律」が施行され、ようやく不正アクセス行為を取り締まる基盤が準備された。また、日本は欧州評議会においてまとめられたサイバー犯罪条約に 2001 年 11 月 23 日に署名し、今批准の準備をしているところである。このように着々とハイテク犯罪対策が整備されていく中で、諸外国のハイテク犯罪法制度の調査、確認を通して、日本における「不正アクセス行為の禁止等に関する法律」の円滑な施行に役立てる目的で、ここに本書を纏め報告するものである。

委員長 清瀬 紀次

執筆者

斎藤 理　　株式会社ラック

白井 雄一郎　　株式会社ラック

内田 法道　　株式会社ラック

鈴木 美保　　株式会社ラック

目次

第 1章　調査の概要

1. 調査の目的

インターネットが世界的に普及した現在、コンピュータ・システムへの不正アクセス行為はネットワークを経由して行われるという性質上、容易に国境を越えて行われてしまう。「インターネットに国境はない」などという見解も語られるほど、ボーダーレスな世界としてインターネットは認識され、広く地球規模で利用されており、それは不正アクセス行為にとっても同じである。ただし、現実には国境がありそれぞれの国家が、それぞれ国内のコンピュータ・ネットワーク、利用者を不正アクセス行為から守るため、さまざまな法制度を整備して対応している。

2000年１月に日本の官公庁の Web サーバが次々に侵入され、コンテンツ改ざんされた一連の事件や、2001年２月に中国のクラッキンググループ（H.U.C.）が日本のサイトに無差別の攻撃を行った事件などは、まだ記憶に新しい。これらは、不正アクセス行為に対する政府、民間の認識を新たにし、「不正アクセス行為の禁止等に関する法律（以下、「不正アクセス禁止法」と略す）」制定のきっかけにもなった。

本書では諸外国におけるハイテク犯罪法制度の整備状況および、最近の不正アクセス手法の手口と傾向を調査し、日本における「不正アクセス禁止法」の円滑な施行に役立てることを目的とする。

2. 調査の方法

⑴ 諸外国におけるハイテク犯罪法制度の整備状況

以下の内容で調査を行う。調査対象としては、先進国の状況を調査するため G8 における不正アクセス対策への取り組みと、近隣アジア諸国でインターネットが普及している国を選び調査を行う。調査の情報源としては、一般に入手可能な情報を元とする。

・調査対象：　G8
　アジア諸国（韓国、中国、インド、マレーシア、シンガポール）

・調査手法：　インターネット、書籍、雑誌等のメディアから情報を収集

・調査項目：　ハイテク犯罪対策への取り組み

ハイテク犯罪に関する法律

－法律名

－公布／施行年月日

－犯罪要件、量刑

なお、諸国の関連法案については部分的に邦訳して紹介している場合があるが、それらは仮に訳しているものであり正式な邦訳でない点に注意されたい。

(2) 不正アクセス行為の傾向と手口

傾向としては、最近多くの報告例がある「ワーム」、「ウィルス」、「Web サイトの改ざん」を取り上げ、また電子商取引サイトにおける「個人情報漏洩」を取り上げる。手口としては、プログラムの制御を奪い、侵入に利用されるバッファ・オーバーフロー、また最近の電子商取引サイトに多く見つかっているクロスサイト・スクリプティング、そしてクライアントを主なターゲットとしている受動的攻撃について調査する。

・調査対象：　傾向（ワーム、ウィルス、Web 改ざん、個人情報漏洩）

手口（バッファ・オーバーフロー、クロスサイト・スクリプティング、受動的攻撃）

・調査手法：　インターネット、書籍、雑誌等のメディアから情報を収集

・調査項目：　傾向（事例、件数、影響など）

手口（仕組み、特徴、影響、事例など）

第 2章　諸外国におけるハイテク犯罪法制度

1. 序

本章では、諸外国におけるハイテク犯罪を取りまく法制度に関して、調査し報告を行う。調査の対象となる国家は G8、アジア諸国とし、主にハイテク産業が盛んで、かつインターネットが普及している国をターゲットとする。これは、情報通信基盤としてのインターネットの普及とともにハイテク犯罪も増加する傾向があるからである。そのため、先進国の例として G8、アジアにおけるインターネット普及が進んでいる国として韓国、インド、マレーシアならびにシンガポールを取り上げて調査を行う。

2. G8 におけるハイテク犯罪対策

(1) サミットにおけるハイテク犯罪対策の流れ

先進国首脳会議（サミット）において、ハイテク犯罪が議題に登るようになったのは国際組織犯罪への対策が機であった。94 年のナポリ・サミットにおいて、国際組織犯罪が初めて取り上げられ、翌 95 年のカナダのハリファックス・サミットにおいて国際組織犯罪対策上級専門家グループの設立が決定された。この「P-8 国際組織犯罪上級専門家会合」は、96 年のリヨン・サミットに「国際組織犯罪に関する 40 の勧告」を提出したことから、「リヨン・グループ」とも呼ばれる。98 年のバーミンガム・サミットでは国際組織犯罪が首脳会合の主要議題の一つとなり、「国際犯罪と薬物に関する声明」が発表された。2000 年の九州・沖縄サミットにおいても、「心の安寧」の中の主要なテーマの一つとして国際組織犯罪が取り上げられ、国際組織犯罪条約及び関連議定書の 2000 年末までの採択に向けた支持の再確認や、ハイテク犯罪対策、腐敗（汚職）対策、司法協力の促進などが盛り込まれた。

リヨン・グループには、司法協力、人の密輸、国連国際組織犯罪条約、ハイテク犯罪、銃器、法執行プロジェクトの 6 つの分科会が設置されており、この中の「ハイテク犯罪サブグループ」は、欧州評議会の「コンピュータ犯罪専門家会合」とともに、主たる国際的フォーラムとなっている。リヨン・グループは、2000 年 5 月、パリにおいて、第 1 回の G8 政府・民間代表者会合を開催し、そこにおいて G8 各国の政府代表者は、主要な通信・新技術関連企業 130 社の代表者と対話を行った。出席者は、新技術の犯罪における使用が通信及びコンピュータ・システムの安全

性を脅かす方法について議論するとともに、あるべき解決策を模索した。2000 年 7 月の九州 ･沖縄サミットにおいて、G8 各国の首脳は、パリ会合で生み出された成果及びモメンタムを歓迎し、民間との対話を促進する必要性を強調した。リヨン ･グループは、官民の対話を進展させるため、2000 年 10 月、ベルリン会合を開催した。ベルリン会合での作業の大部分はワークショップで行われ、政府と民間との協力を妨げる障害の除去、及び、ハイテク犯罪を予防、探知、捜査するための実務的な解決策の追求に重点が置かれた。また、2000 年九州 ･沖縄サミットと2001 年ジェノバ ･サミットの橋渡しとして、2001 年 5 月東京において第 2 回 G8 ハイテク犯罪対策 ･官民合同ハイレベル会合を開いている。

閣僚レベルでは、97 年にリノ米司法長官の呼びかけによりワシントンで開催された G8 司法内務閣僚級会合で「ハイテク犯罪と闘うための原則と行動計画」が採択され、国際捜査共助の必要性が強調された。その後、1998 年 5 月開催のバーミンガム ･サミットでは、サミットとしては初めてハイテク犯罪対策をはじめとする国際組織犯罪対策が主要議題とされた。このバーミンガム ･サミットでは今後各国に求められる法制として、「双罰性」のある法制が言及された。すなわち、犯罪の行為が行われた国と、被害者の住む国の双方の国で刑罰が適用される犯罪行為についてのみ捜査共助が行えるため、相手国と同等の刑罰を規定する法制が各国に求められることになるということである。99 年には、モスクワでハイテク犯罪対策及び国際組織犯罪対策の資金的側面をテーマとする G8 司法内務閣僚級会合が開催されている。

G8 ･サミットによるハイテク犯罪対策（年表）

ナポリ ･サミット 1994 年 7 月 8 日～10 日	サミットにおいて初めて国際的組織犯罪への言及がなされ、1994 年 10 月にナポリで開かれる国際的組織犯罪に関する世界閣僚会議を歓迎するとともに、国際協力の強化が唱えられた。
ハリファックス ･サミット 1995 年 6 月 15 日～17 日	国際組織犯罪対策上級専門家グループの設立が決定され、1996 年のリヨン ･サミットにおいて正式に報告する旨が発表された。
リヨン ･サミット 1996 年 6 月 27 日～29 日	リヨン ･グループによって作成された 40 の勧告を支持、全ての国に推奨する声明を発表。
デンバー ･サミット 1997 年 6 月 20 日～22 日	コンピュータ及び電気通信技術に対して国境を越えて介入するようなハイテク犯罪者についての捜査、訴追及び処罰と、犯罪者の所在地にかかわらず、すべての政府がハイテク犯罪に対応する技術的及び法的能力を有することとなる体制の整備を呼びかける声明を発表。
バーミンガム ･サミット 1998 年 5 月 15 日～17 日	1997 年 12 月にワシントン D.C で開かれた 8 ヶ国司法 ･内務閣僚級会合の成果である「ハイテク犯罪と闘うための原則と行動計画」を採択。これにより、24 時間体制のコンタクトポイント設置やハイテク犯罪捜査強化、国際的な捜査共助のための法制度の整

	備等が促進された。
ケルン・サミット 1999年6月18日～20日	国際組織犯罪及びテロリズムに関するそれぞれの上級専門家グループが行っている作業を賞賛し、両専門家グループに対して、特に組織犯罪に関する国連条約及び議定書についての交渉の早期終結に向けて、引き続き作業を行うよう強く求める旨の声明を発表。
国際組織犯罪対策G8モスクワ閣僚会合 1999年10月19日～20日	バーミンガム・サミット(98年)のコミュニケにおいて、国際組織犯罪に関する閣僚会合を99年モスクワで行うとの提案を歓迎する旨言及されていたが、1999年のケルン・サミットにおいて、同年秋に本会合が開催されることが確認され、開催に至ったものである。ここでは、24時間コンタクトポイントのネットワークが世界的に拡大していることを踏まえ、更なる拡張に努めるよう指示が出され、G8と産業界がインターネット犯罪に関する考え方を共有するための会議の開催の決定がなされた。
G8ハイテク犯罪対策政府・産業界合同会合(於:パリ) 2000年5月15日～17日	G8諸国が初めて政府と民間部門の双方からの上級代表者を一堂に集めた。この会合により、犯罪の防止及び訴追に責任を有する公的機関は、情報技術分野の主要企業130社の代表と対話を開始することができた。
九州・沖縄・サミット 2000年7月21日～23日	2000年5月、パリにおいて開かれたサイバー空間における安全性と信頼性に関する第1回のG8政府・民間代表者会合の結果を歓迎し、2000年10月の合同ベルリン会合を含め、産業界との対話を推進する旨を発表した。
G8リヨングループ・ハイテク犯罪対策に関する政府・産業界合同ワークショップ(於:ベルリン) 2000年10月24日～26日	G8各国より政府、産業界及び国際機関等から約140名程度が参加。2000年5月にパリで開催されたG8ハイテク犯罪対策パリ会議の成果を踏まえ、ハイテク犯罪対策に関し、犯罪者の追跡・特定、ハイテク犯罪の予防、産業界との一層の協力関係の構築の3つのテーマが取り上げられた。会議終了後発出されたG8政府共同プレスリリースでは、ハイテク犯罪対策のために政府と産業界との間の協力の重要性が再確認されると共に、今次会合の成果を踏まえ、2001年5月に東京で第2回ハイレベル会合を開催することが支持された。
第2回G8ハイテク犯罪対策・官民合同ハイレベル会合(於:東京) 2001年5月22日～24日	この会合では、i)データの保存、ii)データの保全、iii)予防及び脅威の分析、iv)電子商取引の保護及びユーザ認証、v)トレーニング、の各問題が話し合われた。会議終了後、G8(政府側)プレスリリースを発表した。その中では、ハイテク犯罪対策における官民間の協力関係を更に強化し、国際協力の促進の必要性が再確認された。

(2) G8各国別のハイテク犯罪法制度の整備状況

欧米各国のハイテク犯罪関連法は、経済協力開発機構(OECD)によって1986年に公表された報告書「コンピュータ犯罪－立法作成の分析」の影響をうけているとされている。以下では、欧米主要6ヶ国の関連法制度について概略する。

(a) アメリカ

米国において、コンピュータに関わる犯罪の法的整備は、連邦法と各州法の二つに分けられる。

連邦法が扱う犯罪は、州際取引（interstates trade）及び国際取引（international trade）に関連するコンピュータ犯罪並びに連邦のコンピュータその他連邦で指定されたコンピュータに関連するコンピュータ犯罪である。そして、この連邦法による法的対処は、大きく分けて二つの制定法によってなされる。一つは、1996 年に改正された「合衆国法典集 第 18 款 第 1 部 第 47 章 1030 条 コンピュータと関係する詐欺及び関連行為」（18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers）であり、あと一つは「合衆国法典集 第 18 款 第 1 部 第 121 章 2701 条 記憶された通信に対する違法アクセス」（18 U.S.C. § 2701. Unlawful Access to Stored Communications）である。前者は、コンピュータ犯罪の中でも「無制限アクセス（unauthorized access to computer）」に対する処罰法規を中心とする刑罰法令であり、後者は、電子通信中のプライバシー侵害に対する処罰法規を含む法令である。特に前者に関しては、アメリカ合衆国連邦におけるウィルス犯罪はそのほとんど全てが「無制限アクセス」としてこの第 1030 条によって対処可能であるとされる。

各州法が取り扱う犯罪は、各州内で発生するコンピュータ犯罪であり、また、連邦によって保護されるコンピュータ以外のコンピュータが関連している犯罪等が処罰対象となるかどうかがこれら各州法によって定められる。各州法の比較において特徴的であるのは、コンピュータ・ウィルスの定義規定の有無である。明確にコンピュータ・ウィルスの定義規定がある州は、カリフォルニア州、メーン州、テキサス州等である。また、明確な形ではコンピュータ・ウィルスの定義規定はないが、これらの存在を所与の前提として、または、コンピュータ・ウィルスと同視可能な破壊的プログラムの定義規定を設けることによって対処している州は、ノースカロライナ州、ネブラスカ州、ミネソタ州、イリノイ州等である。そして、不正アクセス行為の中の一類型としてコンピュータ・ウィルス等によるシステム破壊行為等を処罰対象としている州は、ペンシルベニア州、フロリダ州等、その他の州があてはまる。

(b) イギリス

イギリスにおけるハイテク犯罪に関する法制度は「1990 年コンピュータ不正利用法」（Computer Misuse Act 1990(c.18)）がこれにあたる。この「1990 年コンピュータ不正使用法」第 1

条 (1)によると、コンピュータを作動させる時点において、アクセスが無権限であることを知っていながら、無権限でアクセスする行為が処罰の対象とされている。つまり、無権限アクセスの意図をもってコンピュータを作動させると、実際にアクセスしていなくとも処罰されるとみなされてしまう法律になっている。 また、第1条 (2)によると、何らかの意図をもって特定のプログラム等に行われた不正アクセスだけでなく、結果的に不正アクセスを行ってしまったような場合も、無権限でコンピュータにアクセスする意図があれば本条により罰せられる。

(c) カナダ

1985 年にカナダ議会によってコンピュータに関連した不正行為に対する刑法的対応を図るために犯罪法典 (Criminal Code(R.S.1985,CHAPTER.C-46))に 2 つの規定が新設された。一つは、コンピュータの無権限使用への対応を図った 342 条であり、もう一つはデータの損壊への対応を図った 430 条である。前者の 犯罪法典第 9 部第 342 条 1」(PART IX OFFENCES AGAINST RIGHTS OF PRPERTY,342.1 Unauthorized use of Computer)は、不正かつ無権限に、コンピュータ・システムを直接、間接的に利用すると処罰される法律になっている。 間接的に」とは、教唆や幇助の場合も含まれるということである。また、 犯罪法典第 11 部第 430 条」(PART XI WILFUL AND FORBIDDEN ACTS IN RESPECT OF CERTAIN PROPERTY,430. Mischief)では、生命に危険をもたらす損壊罪については 終身刑」を定めるなど、他国にはない独自性を持っている。

カナダにおいては、特に悪意あるプログラムの配布等に対応することを目的とした規定は存在しない、しかしながら、上記の刑事法において、損壊の犯罪行為及び無権限使用はそうした配布等に対応することが可能であるとされている。

(d) ドイツ

ドイツにおいては、97 年 8 月に 情報通信サービスの大綱条件を規制するための法律 情報通信サービス法)」("Gesetz zur Regelung der Rahmenbedingungen fuer Informations- und Kommunikationsdienste")が施行されているが、これは箇条法で、データ保護、デジタル署名、情報化社会到来に伴う刑法典の改正などを規定している。

実質的に情報通信分野における不法行為を規定しているものとしては、刑法 202 条 a (Strafgesetzbuch (StGB), Funfzehnter Abschnitt. Verletzung des personlichen Lebens- und Geheimbereichs, §202a Ausspahen von Daten)、303 条 a 及び 303 条 b (Strafgesetzbuch (StGB),

Siebenundzwanzigster Abschnitt. Sachbeschadigung, §303a Datenveranderung, §303b Computersabotage）等が挙げられるが、これらは 1987 年の第 2 次経済犯罪対策によって導入されたものである。

しかし、現在情報通信分野における不正行為の取締りはすでに欧州連合の政策が主導となっているため、国内での法制化は関連の EU 指令やガイドラインが成立した場合だけに必要となっている状況である。

(e) フランス

フランスの「刑法典第 1 巻第 3 部第 3 章第 323 条の 1」（Code Penal, LIVRE III - DES CRIMES ET DELITS CONTRE LES BIENS, CHAPITRE III - Des atteintes aux systemes de traitement automatise de donnees, Article 323-1）によると、単なる不正アクセスの他に、不正にコンピュータ・システムの中に留まること及びこれらの未遂、予備、共謀加担する行為も処罰対象になっている法律になっている。

また、「不正情報処理に関する 1988 年 1 月 5 日の法律第 19 号」を中心として、「ソフトウェアの保護に関する 1985 年法（1992 年法改正）」、「情報処理と自由に関する 1978 年法」を加え、包括的な立法措置がとられている。

(f) イタリア

イタリア「1993 年改正刑法」コンピュータ犯罪関連（CODICE PENALE, Libro secondo (Artt.241-649). DEI DELITTI IN PARTICOLARE , Titolo III: DEI DELITTI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA, Capo III: DELLA TUTELA ARBITRARIA DELLE PRIVATE RAGIONI）によると、コンピュータ・ウィルス及びワーム等の不正プログラムを配布すると処罰されるが、積極的に不正アクセスを取り締まる法律にはなっていない。

各国別法体制

国名	法律名	規定
アメリカ	合衆国法典集 第 18 款　犯罪及び刑事手続き 第 1 部　犯罪 第 47 章　詐欺及び虚偽の文言	第 1030 条　コンピュータと関係する詐欺及び関連行為 以下の者は、本条第(c)項に規定するところに従い処罰される。 (1)無権限で、または、授与されたアクセス権限を超過して、コンピュータにアクセスしていることの認識を持ちながら、執行命令もしくは制定法の規定に従い合衆国政府によって国防もしくは外交関係上の理由で無権限の情報開示に対する保護すべきであると決定された情報または 1954 年原子力法第 11 条第 y 項に定義する禁止データについて、入手した情報を保持する行為の手段として、かつ、当該情報が合衆国の利益を侵害する目的で利用され又は外国に有利となるように意欲して通信する目的で利用され得るものであると信ずべき根拠を有しながら、意欲して、通信した者、配達した者、伝送した者、もしくは、通信されるようにした者、配達されるようにした者、伝送されるようにした者、または、その通信、配達もしくは伝送を試みた者、または、それを受信する権限のない者に対して、通信されるようにし、配達されるようにし、もしくは、伝送されるようにした者、または、意欲して、受領権限を有する合衆国の公務員もしくは被用者に対して配達されるべきものを保留した者、もしくは、それが配達されないようにした者
イギリス	1990 年コンピュータ不正利用法	第 1 条コンピュータ･マテリアルに対する無権限アクセス (1)以下の者は、有罪とする。 (a)コンピュータ内に存するプログラムまたはデータにアクセスする意図で、コンピュータに何らかの機能を実行させた場合であって、 (b)その者が得ようとしたアクセスが無権限のものであり、かつ、 (c)その者がコンピュータに当該機能を実行させた時点において、それがコンピュータに当該機能を実行させるものであることを知っていた場合 (2)本条の罪を実行する行為者が有していなければならない意図は、以下のいずれかに向けられたものであることを要しない。 (a)特定のプログラムもしくはデータ (b)特定の種類のプログラムもしくはデータ、または (c)特定のコンピュータ内に保持されているプログラムもしくはデータ。

カナダ	犯罪法典 第 9 部　財産権を侵害する犯罪行為	第 342 条 1 コンピュータの無権限使用 (1)違法に、かつ、権限なく、 (a)直接もしくは間接的に、コンピュータ・サービスを入手した者、 (b)電磁装置、音響装置、機械装置その他の装置を手段として、直接もしくは間接に、コンピュータ・システムの機能を傍受した者、または、傍受されるようにした者、または、 (c)データもしくはコンピュータ・システムに関連して、(a)号もしくは (b)号の犯罪または第 430 条の犯罪を実行する目的で、直接もしくは間接に、コンピュータ・システムを使用した者、もしくは、使用されるようにした者は、 陪審裁判によりうる犯罪として有罪であり、10 年以下の拘禁刑に処し、または、略式裁判によりうる犯罪として有罪である。
	第 11 部 意欲してなされる特定の財産に関する禁止された行為	第 430 条　損壊 (1)意欲して、次のいずれかの行為をした者は、損壊罪を実行するものである。 (a)財産を破壊し、もしくは、毀損すること (b)財産を、危険にすること、使用不能にすること、運用不能にすること、もしくは、無効にすること (c)財産の合法的な使用、享有または、運用に対して、妨害すること、阻害すること、もしくは、干渉すること、または、 (d)財産を合法的に使用し、享有し、もしくは、運用する者に対して、妨害すること、阻害すること、もしくは、干渉すること (1.1)意欲して、次のいずれかの行為をした者は、損壊罪を実行する者である。 (a)データを破壊すること、もしくは、改変すること (b)データを、無意味なものにすること、使用不能にすること、もしくは、無効にすること (c)データの適法な使用を妨害すること、阻害すること、もしくは、干渉すること、または、 (d)データを適法に使用する者に対して、妨害すること、阻害すること、もしくは、干渉すること、または、アクセス権限を有する者のデータへのアクセスを妨げること (2)生命に対する現実の危険を発生させる損壊罪を実行した者は、陪審による裁判により有罪であり、終身刑に処す。
ドイツ	刑法典 第二次経済犯罪対策法	第 202 条 a　データの検知 (1)不正なアクセスに対して特別の保護がなされているデータであって、自己のためのものではないデータを、権限なく、自己または他の者のために入手した者は、3 年以下の

		拘禁刑または罰金刑に処す。 (2)第 1 項の意味におけるデータとは、電子的な方式、電磁的な方式その他人間が直接に知覚できない方式で記憶装置に保存されているもの、または、そのような方式で伝達されるもののみをいう。 第 303 条 器物損壊 (1)他人の物を、違法に、毀損もしくは破壊した者は、2 年以下の拘禁刑または罰金刑に処す。 (2)未遂は処罰する。 第 303 条 a データ偽造 (1)データ 第 202 条 a 第 2 項)を不正に消去し、空白化し、使用不能にし、または、改変した者は、2 年以下の拘禁刑または罰金刑に処す。 (2)未遂は処罰する。 第 303 条 b コンピュータ妨害 (1)他の事業所、他の企業もしくは官庁にとって本質的に重要なデータ処理を、以下の各号に示した方法のいずれかによって妨害した者は、5 年以下の拘禁刑または罰金刑に処す。 1. 第 303 条 a による行為 2. データ処理装置もしくはデータ記憶媒体を破壊し、毀損し、使用不能にし、データを消去し、または、改変する行為 (2)未遂は処罰する。
フランス	刑法典第 1 巻 第 3 部 財産に対する重罪及び軽罪 第 3 章 データの自動処理システムに対する侵害	第 323 条の 1 不法に、データ自動処理システムの全部もしくは一部にアクセスし、または、そこにとどまる者は、1年の拘禁刑または 100、000 フランの罰金刑で処罰する。 この行為の結果として、システムの中に含まれているデータの変更もしくは消去、システム機能の変更が生じたときは、2年の拘禁刑または 200,000 フランの罰金刑で処罰する。 第 323 条の 2 データ自動処理システムの機能を妨害し、または、不調にした者は、3年の拘禁刑または 300,000 フランの罰金刑で処罰される。 第 323 条の 3 データ自動処理システムの中に不正なデータを導入し、または、そこに含まれているデータを不正に消去もしくは変更した者は、3年の拘禁刑または 300,000 フランの罰金刑で処罰される。
イタリア	刑法典 第 2 編 犯罪各則 第 3 章 司法行政に対する犯罪 第 3 節 私権を専断的に保護する犯罪	第 392 条 対物暴行を用いた自己の権利の専断行使 1. 自称の権利を行使する目的で、裁判所に訴えることができるにもかかわらず、物に対する暴行を用いて、自らこれを専断的に満足させた者は、告訴により、1,000,000 リラの罰金刑に処す。 2. 刑法典の効力においては、 物に対する暴行」とは、物を損壊し、変形させ、または、その用途を変更させることを意味する。

		3. 加えて、コンピュータ･プログラムの全部もしくは一部を改変し、変更し、もしくは、削除した場合、または、コンピュータ･システムもしくはデータ･システムの機能を阻害もしくは妨害した場合は、物に対する暴行である。

⑶ G8各国のハイテク犯罪対策の足並み

G8の枠組みであるリヨングループ・ハイテク犯罪サブグループは、通信網へのアクセス記録が簡単に消去され得るため、犯人の追跡・特定に困難が伴うことなどのハイテク犯罪捜査特有の問題に着目し、有効なハイテク犯罪対策及びそのための国際協力の枠組みについて検討してきた。具体的には、24 時間体制の政府コンタクトポイントを設置したほか、ハイテク犯罪捜査促進のための法制度の検討、捜査共助要請に対する迅速な対応、ハイテク犯罪捜査における国境を越えたデータに対するアクセスの在り方等について議論してきた。1999 年 8 月、フランスのライオネル・ジョスパン（Lionel Jospin）首相により、内務省犯罪捜査本部内にハイテク犯罪を取り締まるための中央本部の設立が発表されているが、この機関はG8諸国によって設置されたサイバー犯罪対応のための 24 時間ネットワークにおける連結ポイントの役割も果たしている。

しかしながら、例えば2000年5月のパリ会議において、フランスが国際サイバー警察を設置するという米国提案を拒否、サイバー犯罪対策はユーロポールの管轄であると主張するなど、G8 のレベルでサイバー犯罪対策問題の足並みが揃わない面もある。また、産業界側からの反応として、サイバー犯罪対策に関して政府や関連当局にはそれに対応しうる十分な知識・技術を持っていないとの不信の声もあがっている。これは政府による性急な関連法規の制定に対する産業界からの警告となっている。

「欧州サイバー犯罪条約」は、リヨン・グループではなく、欧州評議会の「コンピュータ犯罪専門家会合」の手によるものであり、また、条約としては構成国以外にも署名開放されることから、G8・サミット主体のハイテク犯罪対策の流れも変化してくることが予想される。

3. 韓国におけるハイテク犯罪対策

⑴ 韓国におけるハイテク犯罪対策の流れ

韓国では、警察庁が1995年ソウル地方検察に情報犯罪捜査センターの発足させ、現在大検察庁が「コンピュータ犯罪担当捜査チーム」を運営しており、地方検察庁では「コンピュー

タ犯罪担当検査」を運営中である。警視庁は1995年ハッカー捜査担当チームを発足させ、現在は 甲サイバーテロ対応センター」として拡大、改編し運営されている。一方、国際犯罪関連情報を集める国家情報院では、1998年 8月国家 (公共)機関電算網保安事故処理を担当する 情報保安 119(NISSC, National Information Security Service Center)」を設置、運営している。以上は政府の取り組みであるが、民間においては韓国情報保護センターが1998年 韓国電算網侵害事故対応支援チーム(CERTCC-KR)」を発足させ、検察及び警察がハッカーの取締りを支援している。

それにもかかわらず、サイバー犯罪は、増加し続けているが、韓国情報保護振興院から提供する2001年 12月のハッキング事故の受け付け関連統計を参考すると、増加し続けているのが分かる。

参考資料」

2001年 12月侵害事故の受け付け及び処理状況

侵害事故の受け付け及び処理状況

(a) 事故の受け付け及び処理現況

	事故の受け付け	被害機関 (国内/国外)
件数	422	384/ 38

12月のハッキング事故の特徴

- 12月に届けられた事故の件数は 384件で、前月と比較し12%増加している。
- 2001年のハッキング事故の累積は 5333件で、1ヶ月平均にすると約 444件が届けられ、これは2000年の事故件数と比べると274%の増加率である。
- このようにハッキング事故が急増した原因は、ネットワーク上のシステムを攻撃するインターネットワームの発生とも関連があると思われる。

(b) 現在の被害状況

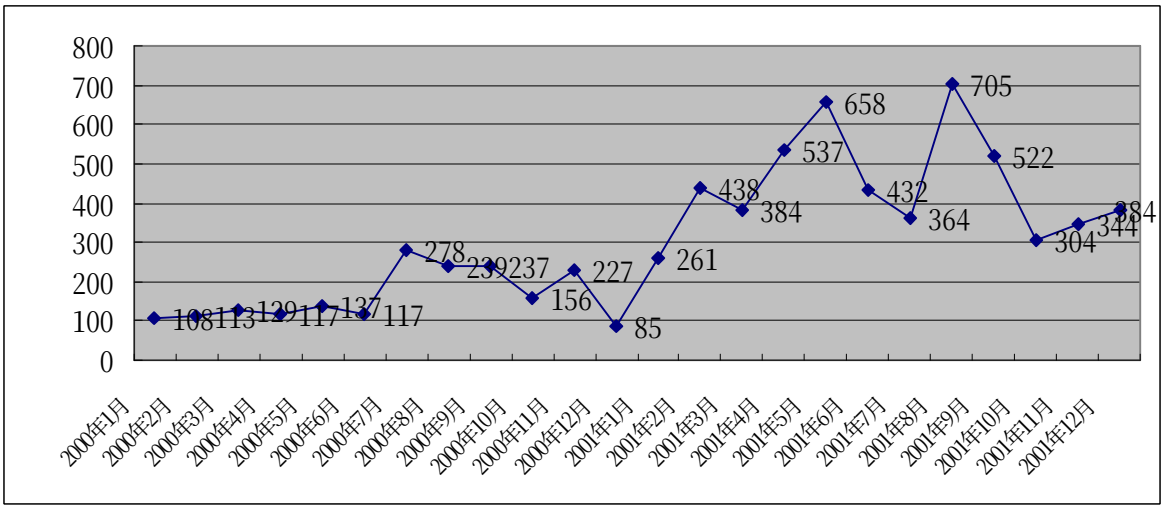
ハッキングによる被害状況（年別）

年度	'96	'97	'98	'99	'00	'01.12 月	全体
件数	147	64	158	572	1943	5333	8217

ハッキングによる被害状況（月別）

月	'00.1	'00.2	'00.3	'00.4	'00.5	'00.6	'00.7	'00.8	'00.9	'00.10	'00.11	'00.12	合計
件数	108	113	129	117	137	117	278	239	237	156	227	85	1943

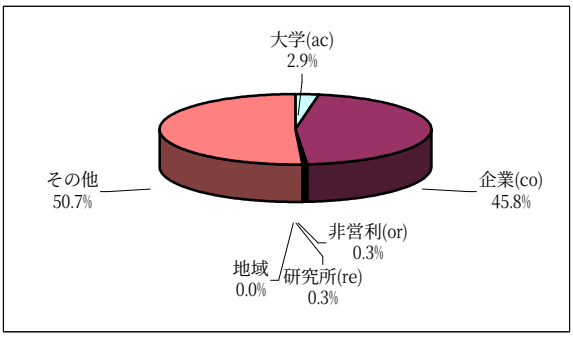
月	'01.1	'01.2	'01.3	'01.4	'01.5	'01.6	'01.7	'01.8	'01.9	'01.10	'01.11	'01.12	合計
件数	261	438	384	537	658	432	364	705	522	304	344	384	5333



(c) 事故の分析

被害を被った機関の数

	被害を被った機関	
区分	機関の数	割合（%）
大学(ac)	11	2.9
企業(co)	176	45.8
非営利(or)	1	0.3
研究所(re)	1	0.3
地域	0	0
その他	195	50.7
合計	384	100



ハッキングの手法

区分	件数	備考
ユーザの盗用	33	ユーザアカウントを盗用
ソフトウェアのバグ	0	－
バッファ・オーバーフロー	4	named/bind 等の脆弱性を利用
構成／設定のミス	1	ユーザ権限設定ミス
悪意のあるプログラム	97	Nimda ワーム、Windows 用トロイの木馬
プロトコルの脆弱性	0	－
使用不能攻撃	1	サービスを提供できなくさせる
メール関連の攻撃	1	spam メール等による攻撃
脆弱性の調査	247	named/bind,ftpd,rpc の弱点をスキャン
ソーシャルエンジニアリング	0	－

国内・外関係

区分	件数
国内→国内	11
国内→国外	38
国外→国内	18
国外→国内→国外	3
不明	352
合計	422

＊　”国内→国外 ”は被害を被った機関が国外にあるため、国内のハッキングの合計からは除く

不法行為別の区分

区分	件数	備考
侵入の試み	353	弱点に対する情報収集などを利用した侵入の試み
不正侵入	30	一般及び管理者権限獲得
情報漏洩	0	重要資料の流出
データ改ざん／削除	0	資料変造・削除
不正資源の使用	0	被害システムの資源を無断使用
ホームページ改ざん	0	ホームページ改ざん
システム破壊	0	システム破壊
システムエラー	0	システムエラー
使用不能攻撃	1	使用不能攻撃

被害 OS 別の区分

OS	被害件数	OS	被害件数
Linux	44	HP-UX	-
Solaris	3	DEC/IRIX	-
Windows95/98	107	CISCO	-
Windows NT/2000	36	AIX	-
不明	194	DIGITAL UNIX	-

⑵ 韓国におけるハイテク犯罪法制度の整備状況

現在韓国では、世界の情報化の流れに合わせるために急いで情報通信環境を整え、物理的情報通信のインフラ施設の構築と準備に集中したため、不正アクセス行為等の情報化の負の側面に対応する法制度は立ち遅れていた。特に統計資料で確認したように急増する不正アクセス行為や、コンピュータ・ウィルスの配布などの様々な電子的な侵害行為に対して、体系的かつ総合的な対応が可能な法律の整備がなされていなかった。、従来の電気通信基本法、情報化促進基本法、情報通信網利用促進などに関する法律、国家情報院法、保安業務規定等は主に物理的施設に対した保護対策を中心に規定しているだけで、電子的侵害行為に備えて主要情報通信基盤施設を保護するための、国家的な予防対策を樹立できる基本法は存在していなかった。

韓国政府は、このような問題点に対する認識のもと、また主要情報通信基盤施設を保護するために、新しい法律の必要性が民間で広がるにつれ、情報通信部は情報通信基盤整備に伴う負の側面に対処するための法律制度の整備を推進し、2001年1月に 情報通信基盤保護法」を新たに制定し、 情報通信網利用促進などに関する法律」の改正を行った。

情報通信基盤保護法」は、外国法制の研究・分析、関係機関・専門家の意見を参照しながらな、数年間の準備を通じて情報通信部が作成し、様々な電子的侵害行為から主要情報通信基盤施設を効果的に保護するための法律である。

情報通信網利用促進及び情報保護などに関する法律」は、従来の 情報通信網利用促進などに関する法律」を改正したもので、個人情報保護に関する一般法律として生まれ変わった。改正された法律では、個人情報保護の義務条項を適用する対象者としてオフライン事業者まで拡大することで、個人情報処理の委託などによる事業者の責任を強化し、消費者の自己情報に対するアクセス権と拒否権を保障している。また、14 歳未満の子供の個人情報保護制度を一新し、さらに 個人情報紛争調整委員会」を設立して個人情報に関する争いを迅速に解決でき

るような制度を設けた。さらに、① 「内容選別ソフトウェア」の開発・普及、②青少年保護法上の青少年有害媒体の情報に対する青少年有害媒体の表示義務を付加、③サービス拒否攻撃、サイバー上の他人の名誉を損なう行為等のハイテク犯罪に対する処罰の根拠を規定した。

それでは、「情報通信基盤保護法」について詳しく説明していく。

(a) 情報通信基盤保護法の推進経過

刑法、情報通信網利用促進及び情報保護に関する法律などに不正アクセス、ウィルス配布行為に対して一部処罰条項があるが、新たな電子的侵害行為から主要情報通信基盤施設を保護するための事前予防、事後対応を規定する法律はない。そのため、不正アクセス行為、ウィルス配布などの電子的侵害行為から主要社会基盤施設を運営する情報通信システムを保護するため関連法律として、2000 年 2 月開かれた「サイバーテロ防止関係長官会議」で「情報通信基盤保護法」を制定することを決定し、下記のような日程を経て情報通信基盤保護法を制定・公布及び施行した。

情報通信基盤保護法推進経過

2000 年 2 月： 国務総理の主催で開かれた「サイバーテロ防止関係長官会議」で「情報通信基盤保護法」制定の推進を決める

2000 年 9 月： 規制改革委員会 新設規制の審査

2000 年 10 月： 法制所 法案審査及び党政協議

2000 年.11 月： 法案 次官・国務会議の審議・議決

2000 年 12 月： 法案 国会本会議議決

2001 年 1 月： 情報通信基盤保護法制定・公布（法律第 6383 号）

2001 年 7 月： 情報通信基盤保護法施行及び施行令公布（大統領令第 17308 号）

2001 年 8 月： 情報通信基盤保護法施行規則公布・施行（情報通信部令第 115 号）

(b) 情報通信基盤保護法の概要

情報通信基盤保護法は主要情報通信基盤施設の保護を主目的として制定された法律である。その主要な部分を抜粋、要約する。

第 3 条

主要情報通信基盤施設の保護を目的とした、政府の対応体制を構築するために、国務総理の下に情報通信基盤保護委員会を設置する

第 5 条／第 6 条

主要通信基盤施設を管理する機関の責任者は、定期的に所管施設に対する弱点の分析・評価、保護対策を樹立・施行し、主要情報通信基盤施設を管理する中央行政機関の責任者は、所管分野別の主要情報通信基盤施設保護計画を樹立・施行する

第 7 条

国家安全保障に重大な影響を及ぼす道路・地下鉄・空港・電力施設など、主要情報通信基盤施設の管理機関の責任者は、国家保安業務を行う機関の責任者にまず技術的支援を要請する。ただし、金融情報通信基盤施設など個人情報がデータベース化されている情報通信基盤施設に対しては、国家保安業務を行う機関の責任者は技術的支援を行えないこととし、その他の主要情報通信基盤施設に対しては大統領令が定める国家機関の責任者、または専門機関の責任者に技術的支援を要請する

第 8 条

中央行政機関の責任者は情報通信基盤保護委員会の審議を経て、電子的侵害行為からの保護が必要と認められる情報通信基盤施設を主要情報通信基盤施設として主要施設に指定する

第 13 条／第 14 条

主要情報通信施設を管理する機関の責任者は所管施設が侵害事故によって破壊されたことを判明した場合、これを関係機関などに通知して被害拡散防止のための対策を行う

第 17 条

情報通信部長官は、主要情報通信基盤施設を管理する機関の同施設に対する弱点を分析、評価、および保護対策の樹立を支援するために情報保護専門会社を指定する

(c) ハイテク犯罪に関連する法律

・不正アクセス、盗聴等

情報通信網利用促進及び情報保護等に関する法律

第 49 条（秘密等の保護）

「だれでも情報通信網によって処理、保管、または伝送される他人の情報を毀損すること、他人の秘密を侵害・盗用または漏洩してはならない」

同 第 62 条

「第 49 条の規定を違反して他人の情報の毀損し、他人の秘密を侵害、盗用し、または漏洩した者は、5年以下の懲役または 5千万ウォン以下の罰金とする」

この条文は、韓国科学技術研究所（KAIST：Korea Advanced Institute of Science and Technology）のネットワークが侵入された事件等で適用された規定である。他人の ID、パスワードを利用してコンピュータ・システムに侵入し情報を入手したり、情報を変更したり、または盗聴したりする行為はこの法律によって犯罪とされる。また、同 第 48 条は「だれでも正当なアクセス権限なく、または許容されたアクセス権限を超過して、情報通信網に侵入してはいけない。」と規定しており、違反した場合には 3 年以下の懲役または 3 千万ウォン以下の罰金にすることを規定している。

・主要通信基盤への使用不能攻撃

情報通信基盤保護法

第 28 条第 1 項

「第 12 条の規定を違反して主要情報通信基盤施設を攪乱・麻痺または破壊した者は 10 年以下の懲役または 1 億ウォン以下の罰金にする」

と規定し、「情報通信基盤施設（主要社会基盤施設の運用と関連されている制御・管理システムと情報通信網利用促進等に関する法律第 2 条第 1 号の規定による情報通信網）」への犯罪を特別に扱っている。また、未遂犯の処罰についても規定されている（同条第 2 項）。

・侵害される情報の種類による他の処罰規定

犯罪行為により入手される情報の種類により、関連する様々な処罰法が存在する。侵害された秘密の種類によって適用される構成の要素は以下のようになる。

①国家機密情報の場合：スパイ罪（刑法 第98条 第1項）

②公務上の秘密情報場合：秘密侵害罪（刑法 第140条 第3項）

③個人の秘密情報の場合：秘密侵害罪（刑法 第316条 第2項）

④信用情報コンピュータ・システムの情報の場合：信用情報検索罪（信用情報保護法上：第32条 第11項）

⑤貿易業者等の秘密情報の場合：貿易秘密侵害罪（貿易業務自動化促進法 第26条 第3項）

⑥軍事機密の場合：軍事機密探知収集罪（軍機密保護法 第11条）

4. 中国におけるハイテク犯罪対策

⑴ 中国のハイテク犯罪対策に関連する取り組み

中国では、インターネットはハイテク産業・通信産業の一環として重要視されている技術のひとつである。中国の特徴として新聞やニュースに関わるソフトやコンテンツの制作や発信については、基本的に国家や国有企業が独占状態を維持しているため、外国資本・外国事業体からの参入を制限しているが、インフラあるいはハイテクについては外国資本の参入は歓迎されており、中国政府から様々な優遇措置が与えられている。インターネット事業（産業）のような通信・情報関連の分野に関しては、国家安全が脅かされるかどうかが制限項目か奨励項目かの判定基準になっている。

⑵ インターネットに対する法的規制

中国のインターネットに関する法律は2つある。1つは、1994年2月18日、中国国務院が公布した「コンピュータ情報システム安全保護条例」であり、もう1つは1996年2月1日、同様に中国国務院が公布した「コンピュータ情報ネットワークの国際的接続に対する管理についての暫定規定」である。この2つの法規は、中国のインターネットに対する法的規制の基本を構成したものである。この2つの法規及び関連規則をまとめて見れば、中国のインターネットに関する

法的規制は以下のような特徴がある。(以下条文は、「コンピュータ情報ネットワークの国際的接続に対する管理についての暫定規定」からの抜粋)

(a) プロバイダの視点から

第 6 条

「コンピュータ情報ネットワークが直接に国際的接続を行うときは、郵電部国家公用電信網が提供した国際ポート通信路を使用しなければならない。いかなる単位と個人といえども, 自ら別の通路を建設または使用して国際的接続を行ってはいけない。」

コンピュータ・ネットワークのインターネットへの新規接続（いわゆる商業ネット）は、原則として、郵政省の管理している国家公用電信ネットを経由して行わなければならない。 プロバイダとしてコンピュータ・ネットワークを作る場合は、加盟先インターネットの主管官庁の許認可を受けなければならない。許認可の手続きをする際、コンピュータ・ネットワークの性質、運営範囲、メインコンピュータの所在地等の資料を提供しなければならない。 プロバイダについては、中国語では「接入単位」という法律用語が使われているが、その定義から見れば、必ずしも商業ネットのプロバイダに限るとは言えない。つまりインターネット接続業務を目的とするものならば、全部この「接入単位」の範囲に入るわけである。プロバイダ（接入単位）は、省級レベル以上の人民政府の警察部署に届出をしなければならない。

(b) 国家政策の視点から

第 8 条

「接入接続は, 相互接続を通じて国際的接続を行わなければならない。接入接続を建設しようとする単位は, 相互接続の主管部門あるいは主管単位の審査と許可を得なければならない。審査及び許可に際しては, そのコンピュータ情報ネットワークの性質と適用範囲及び主な機械が必要とするアドレス等の資料を提供しなければならない。」

中国ではインターネットに主管官庁が強く関与していることが特徴である。国務院に設置されている経済情報化指導グループ（中文：経済信息化領導小組）が、総責任者としてネット

ワークの国際的接続に関する重大な問題を調整して解決している。この経済情報化指導グループは、郵政省(中文：郵電部)、電子工業省（中文：電子工業部）、文部省（中文：国家教育委員会）及び中国科学院、それぞれの各関係官庁の責任担当者から構成され、管轄範囲にあるインターネット分野を管理している。また、新規のインターネット関連のインフラを建設する場合は、国務院の許認可を受けなければならない。郵政省の主導のもと、インターネット関連事業を統括しようという現行法規制の特徴がある。インターネットを通信事業の一環として統括することによって、安全性を確保する一方、国営事業としての収益を獲得することが目的である。郵政省で統括する第一の目的は、国益に有害な情報源を排除することであり、又インターネット関連事業の収益をある程度独占することができるからである。

(c) ユーザの視点から

第 10 条

「個人，法人その他組織（以下利用者と称する。）は，コンピュータまたはコンピュータ情報ネットワークを使用して国際的接続を実行しようとするときは，接入接続を通じて国際的接続を行わなければならない。」

コンピュータ・ネットワークの安全管理に関しては、警察省（公安部）が責任を持っている。個人、法人その他の組織は、ユーザとしてインターネットに接続する場合、プロバイダ(接入単位)を通して行わなければならない。プロバイダに加盟したら自由にインターネットにアクセスすることができる。加盟する際は、身分証明書（又はパスポート）を提示しなければならない。加盟後、警察当局の担当窓口に行って届出をしなければならない。

(3) ハイテク犯罪に対する規制

中国のハイテク犯罪に関する法律は 2000 年 12 月 28 日、第 9 期全国人民代表大会常務委員会第 10 回会議で可決された「インターネットセキュリティ保護の決定」である。

『インターネットセキュリティ保護の決定』

我が国のインターネットは、国の率先した提唱と積極的推進により、経済建設と各事業において日増しに広く運用され、人々の生産、事業、学習、生活様式にすでに大きな変化を

もたらし、今後も我が国の国民経済と科学技術の発展、社会サービスの情報化のスピードアップに重要な役割を担うであろう。同時に、インターネット運営の安全と情報の安全をいかに保障するかという問題が社会全体の注目を集めている。その利点を生かし弊害を取り除き、我が国のインターネットの健全な発展を促し、国家の安全と社会の公共利益を保護し、個人、法人、その他組織の合法的権益を守るため、特に以下の決定を行う。

第 1条　インターネット運営の安全を保障するため、以下の行為があり犯罪を構成するものは、刑法の関連規定に照らし刑事責任を追究する。

⑴国家事務、国防建設、先端科学技術の領域のコンピュータ情報システムに侵入したもの。

⑵故意にコンピュータ・ウィルスなどの破壊的プログラムを製作、伝播し、コンピュータ・システム及び通信ネットワークを攻撃、コンピュータ・システム及び通信ネットワークに損害を与えたもの。

⑶国家規定に違反し、故意にコンピュータ・ネットワークまたは通信サービスを中断させ、コンピュータ・ネットワークまたは通信システムが正常な運営をできなくしたもの。

第 2条　国家の安全と社会の安定を守るため、以下の行為があり犯罪を構成するものは、刑法の関連規定に照らし刑事責任を追究する。

⑴インターネットを利用してデマ、誹謗またはその他の有害情報を発表、伝播し、国家政権転覆、社会主義制度打倒を扇動、または国家分裂、国家統一の破壊を扇動したもの。

⑵インターネットを通じて国家の機密、情報または軍事機密を盗み、漏洩したもの

⑶インターネットを利用して民族的憎しみ、民族差別を扇動、民族の団結を破壊したもの。

⑷インターネットを利用して邪教組織を組織、邪教組織成員と連絡し、国家の法律、行政法規の実施を破壊したもの。

第 3条　社会義市場経済秩序と社会管理秩序の保護のため、以下の行為があり犯罪を構成するものは、刑法の関連規定に照らし刑事責任を追究する。

⑴インターネットを利用して偽造製品を販売、または商品、サービスに虚偽の宣伝をしたもの。

⑵インターネットを利用して他人の商業信用と商品信用に損害を与えたもの。

⑶インターネットを利用して他人の知的所有権を侵したもの。

⑷インターネットを利用して証券、先物取引に影響する、またはその他金融秩序を乱す虚偽の情報を捏造し伝播したもの。

⑸インターネット上でわいせつなサイト、ページを立ち上げ、わいせつサイトへのリンクサービスを提供、またはわいせつな読み物、映像、音声、画像を伝播したもの。

第 4条　個人、法人、その他組織の人身、財産など合法的権利を保護するため、以下の行為があり犯罪を構成するものは、刑法の関連規定に照らし刑事責任を追究する。

⑴インターネットを利用して他人を侮辱、または事実を捏造して他人を誹謗したもの。

⑵不法に他人の電子メールまたはその他データ資料を盗み、改善、削除し公民の通信の自由と通信のプライバシーを侵したもの。

⑶インターネットを利用し窃盗、詐欺、恐喝を行ったもの。

第 5 条　インターネットを利用して本決定の第 1条、第 2条、第 3条、第 4条の行為以外のその他の行為があり犯罪を構成するものは、刑法の関連規定に照らし刑事責任を追究する。

第 6 条 インターネットを利用して違法行為を行い、社会治安管理に違反するが、それでも罪を構成しないものは、公安機関が『治安管理処罰条例』に照らし処罰を与える。その他法律、行政法規に違反するが、それでも犯罪を構成しないものは、関連の行政管理部門が法に照らし行政処分を与える。直接責任を負う主管者とその他直接の責任者に対しては、法に照らし行政処分または紀律処分を与える。インターネットを利用して他人の合法的権益を侵し、民事侵権を構成するものは、法に照らし民事責任を負う。

第 7条 各級人民政府及び関係部門は積極的措置を取り、インターネット運用とネットワーク技術普及の促進において、ネットワークセキュリティ技術の研究開発を重視、支持し、ネットワークセキュリティ保護能力増強を行わなければならない。関係主管部門はインターネット運営の安全と情報の安全に対する宣伝教育を強化し、法に照らし有効な監督管理を実施し、インターネットを利用した各種違法行為を防犯、阻止し、インターネットの健全な発展のために良好な社会環境を創造しなければならない。インターネット業務に従事する事業団体は法に照らし活動を行い、インターネット上で違法犯罪行為と有害情報を発見したときは、措置を取り、有害情報を阻止し、直ちに関係機関に報告をしなければならない。いかなる事業団体と個人もインターネットを利用するときは、法律を守り、各種違法犯罪行為と有害情報を排除しなければならない。人民法院、人民検察院、公安機関、国家安全機関はそれぞれの職務を指揮し、互いに協力して、法に照らしインターネットを利用した各種犯罪活動の撲滅を行わなければならない。全社会の力を動員し、全社会の共同の努力によって、インターネット運営の安全と情報の安全を保障し、社会主義精神文明と物質文明の建設を促進しなければならない。

普通のユーザを含めるインターネット関連業務に携わる組織や個人は、インターネットを利用して国家の安全に危害を加え、国家の秘密を漏洩するような犯罪活動をしてはいけないし、また社会の治安状態を妨げるような情報やポルノ情報を制作・閲覧・複製・発信してはいけない。またコンピュータ情報システム安全保護条例によれば、コンピュータ情報システムを損なうウィルスやデータを故意に送り込む場合は、行政罰が科される。 コンピュータ・ウィルスを故意に制作・発信する場合への対応は他国と変わらないが、それ以外の規制内容については、中国独

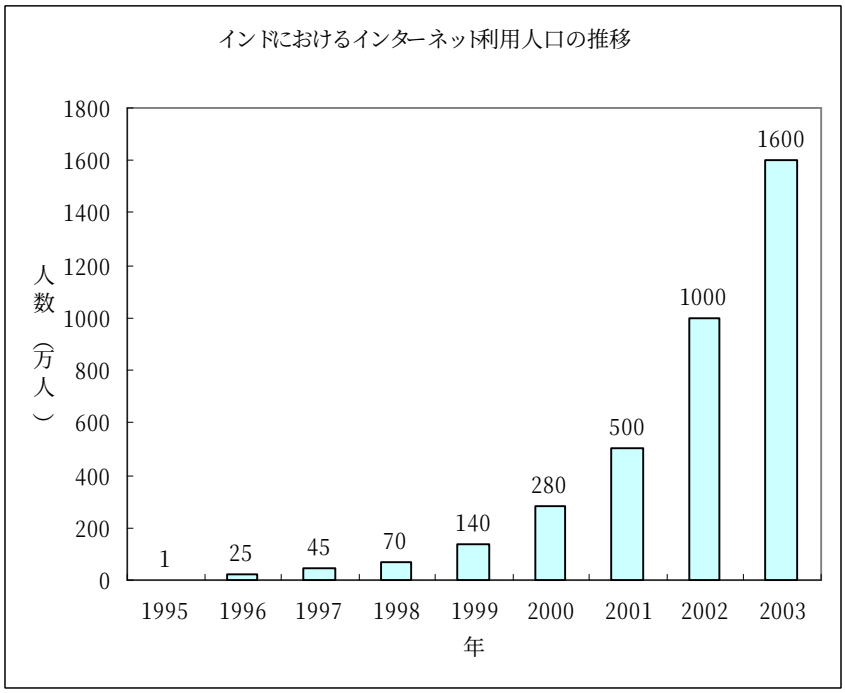
自の規制である。特に社会の治安状態を妨げるような情報やポルノ情報を閲覧していけない（アクセスしてはいけない）というような規定は、実際には規制が難しい。例えば、ホームページの内容を知らずに偶然アクセスしたところ、表示された内容がポルノ関係であるというような場合も想定されるため、技術的に禁止することも法的に禁止することも難しい。法律として明文化してあるものの、明確な規準はまだできていないというのが現状のようである。今後は判例が基準となっていくのであろうが、現在のところ中国で公開された判例は少ないようである。中国の法律の特徴はユーザにとって不利益な事柄を取り締まるよりも、国家にとって不利益な事柄を取り締まる方に重点が置かれている点であろう。

5. インドにおけるハイテク犯罪対策

(1) 法整備の経緯

1990 年代後半からインドでは、国策として情報技術産業を強化するために、政策がいくつも施行されるようになった。1998 年 5月には「情報技術・ソフトウェア開発タスクフォース」（National Task Force on Information Technology & Software Development）を、インドにおける情報技術の急速な発展を促進するために設置した。同タスクフォースはアクション・プランと呼ばれる提言を行い、政府もそれを実行し、インドの情報技術産業は飛躍的に発展した。同時に、インドにおけるインターネット人口も爆発的に増加した。（表）

情報技術産業の発展とインターネット人口の増加に伴って、若干遅れ気味であった法律、特に電子商取引に関する法律を整える必要性が出てきた。そこで、インド政府は電子商取引の基本的な枠組みを整えるべく、1999 年 12 月に情報技術法案（the information technology bill 1999）を国会に提出した。その法案は、2000年5月に国会に承認され、同年10月に施行された。これには、電子商取引が増えるにつれ増加するであろうコンピュータ犯罪に対応するために、ハッカーに対する規制や犯罪の定義などが折り込まれた。



⑵ インドにおけるハイテク犯罪法制度

情報技術法ではハイテク犯罪について規定している。管理者の許可なくコンピュータ・システムにアクセスする行為、データを盗む行為、ウィルスを作成する行為、破壊行為、成りすましてアクセスする行為をシステムに損害を与える行為として犯罪として定め、1000 万ルピー以下の罰金を被害者に支払うとされている。

実際の条文を以下に掲げるが、その前に条文内で利用される用語の説明をしておく。

① コンピュータ汚染物質とは以下のような行為をコンピュータに指示するために作られたプログラムである

(a) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内の情報を許可なく転送・記録・破壊・修正するもしくは常駐するプログラム、

(b) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワーク内における権限をあらゆる手段によって奪うプログラム

② コンピュータ・データベースとは、

(a) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークにおいて使うことを目的として作られ、

(b) 文章や画像、音、映像などの形式によって保存され、

(c) あるいは保存されている情報・知識・事実・概念・命令を表現しているものとする。

③ コンピュータ・ウィルスとは、コンピュータ資源の能力を低下・使用不可能・破壊するコンピュータ命令・情報・データ・プログラムのことである。また、上記のプログラムをコンピュータで実行する、もしくは、他のイベントがそのコンピュータ内で実行された時自らを他のコンピュータに感染させるものを意味する。

④ 損害とは、何らかの手段により、コンピュータ資源を破壊・改変・混乱・削除・追加・修正・再配置させることを意味する。

不正アクセス行為を処罰する旨規定されている情報技術法の関連条項を部分的に仮訳する。

第 43 条 コンピュータ、あるいはシステムに対する傷害を与えた場合の刑罰
コンピュータあるいはコンピュータ・システムあるいはコンピュータ・ネットワークの管理者やそれらに対して権限のあるものの許可なく、

(a) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークに対してアクセスする
(b) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークあるいは全てのリムーバブル・ディスクからデータベースや情報をダウンロード、コピー、もしくは取り出す
(c) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークにコンピュータ・ウィルスを侵入させるもしくはその原因を作る
(d) コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークに存在するデータベースあるいはその他のプログラムに損害を与えるもしくはその原因を作る
(e) コンピュータあるいはコンピュータ・システムあるいはコンピュータ・ネットワーク、データベースあるいはそれらにある他のプログラムを物理的に壊すもしくはその原因を作る
(f) 管理者や適正な権限のある人物のコンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークに対するアクセスを行わせない、もしくはその原因を起こす
(g) 法律や規制により違反行為であると定義されている手法により、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークに不正にアクセスする者の行為を助長し、協力す

る。

(h) 他人のパスワードなどを使用して、コンピュータ、コンピュータ・システムもしくはコンピュータ・ネットワークに対して操作、改ざんなどを行う。

以上の行為を通して、コンピュータ・システムに傷害を与えた場合、1000 万ルピー以下の罰金を被害者に払う。

第 44 条 情報提供を怠った場合の規定

もし、第 43 条の行為を犯したものは、

(a) コンピュータの管理者に情報提供のために文書や報告書などを提出する、または、管理者が同等のものを提供することを怠った場合、10 万 5 千ルピー以下の罰金を払う。

(b) どのような報告、または情報をも保管し続け、特定期間冊子やその他の文書を他者に提供することを怠った場合、その行為が継続する間毎日 5000 ルピー以下の罰金を払う。

(c) 会計簿、またはその記録の保持、またそれと同等の行為を怠たりることで損害を出した場合は、その行為が継続する間、毎日 1 万ルピー以下の罰金を払う。

第 45 条 余罪

本法令において定義された複数の犯罪行為に及んだにも関わらず、別々に罰則が与えられなかった場合、被害者への 2 万 5000 ルピー以下の損害賠償、あるいは 2 万 5000 のルピー以下の罰金を払うものとする。

第 65 条 コンピュータ・ソース文書の不正使用

コンピュータのソースコードが法律によって保存を命ぜられている場合に、意図的に、コンピュータ、コンピュータ・プログラム、コンピュータ・システム、もしくはコンピュータ・ネットワークで用いられるコンピュータのソースコードを隠蔽・破壊・または改変した者は 3 年以下の懲役、もしくは 20 万ルピー以下の罰金もしくはその両方の刑罰をうける。

「コンピュータ・ソースコード」とは、プログラムやコンピュータのコマンドやデザイン・レイアウトやコンピュータ・リソースのプログラムの詳細が列挙してあるものである。

第 66 条 コンピュータ・システムへのハッキング

意図的に、公もしくは特定の個人に損害を与えることを認知しておきながら、あらゆる手段、例え

ばハッキングなどの犯罪行為により、コンピュータ・リソースに存在するあらゆる情報を破壊・変形・消去する、もしくはその価値や有効性を減退させ、悪影響を与えた罪を犯したものは 3 年以下の懲役あるいは 20 万ルピー以下の罰金を、もしくはその両方の刑罰を与えられる。

第 67 条 電子データにおける猥褻情報の公開
淫らなものへの興味を引き付けるために、そのような画像や映像を出版、転送、電子形式で公開する。あるいは、その影響によって他人がそのような淫らな写真や映像などへの興味を増幅させ、入手させるように仕向けた者は、初犯では最大 5 年の懲役と最大 10 万ルピーの罰金を払う。また、2 回目以降は最大 10 年の懲役と20 万ルピーを払う。

⑶ 情報技術法が適用された事例の紹介
上記法律が実際に適用された事例としては、2 人のインド人コンピュータ・インストラクターが、インドで最大の銀行であるインド連邦銀行や他の代表的な銀行に侵入しようとした罪で起訴された事件があげられる。コンピュータ・トレーニング事業を行っている Aptech 社に勤務していた Manoj Singhania とPrakash Yadav の両名が、2001 年 1 月 11 日に逮捕された。
容疑は、マイクロソフト社とVidesh Sanchar Nigam 社（国際電話でインド1のシェアを持つ企業）の名前を使って speed.exe というファイルを添付した電子メールをたくさんのメールアドレスに送信した疑いである。添付されたファイルを実行すると、データやパスワードが容疑者のメールアドレスに送信される仕組みになっていた。両名は、インド情報技術法により3年以内の懲役及び4300 米ドル（20 万ルピー）の罰金の刑罰が求刑されている。ただし、警察、検察、裁判所におけるコンピュータへの利用、理解が進んでいない現状で、ハイテク犯罪について正しい解釈、判決を出すことは困難であろうと思われる。

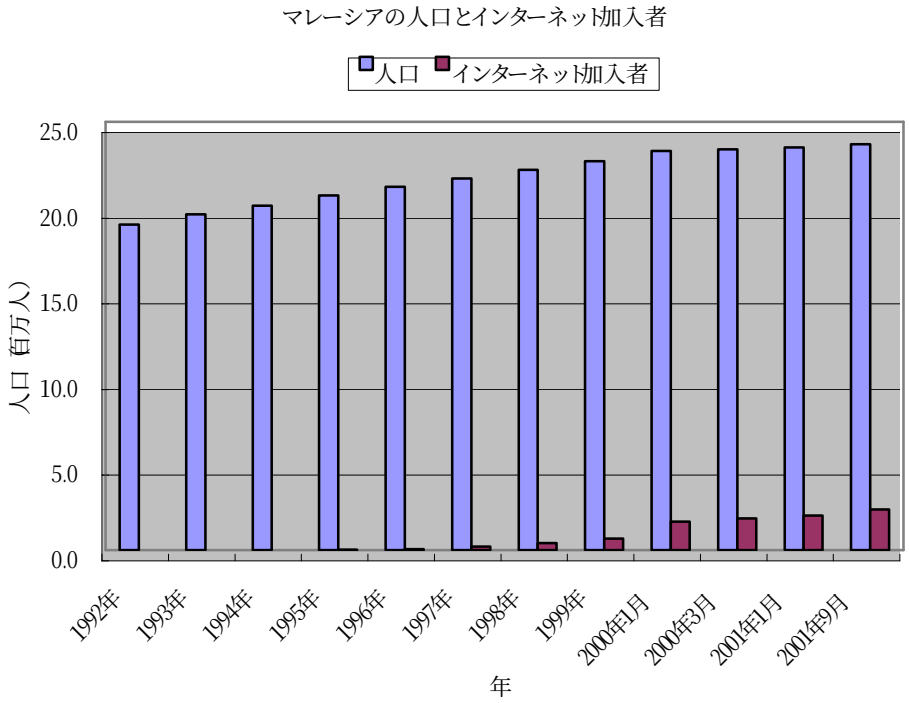
6. マレーシアにおけるハイテク犯罪対策

⑴ 法整備についての背景と経緯
かつてマレーシアは、スズやゴムなどの一次産品の輸出に依存する途上国の一員だった。マレーシアは、マレー系、中国系、インド系などの民族の混在する多民族国家であり、経済格差などでの理由で不安定な時期があった。しかし、1980 年代後半には、外資規制の緩和策や

周囲の状況の変化により、日本などからの直接投資の急増を呼び込み、輸出型産業の拡大が進んだ。1991 年には、2020 年までに先進国の仲間入りを目指して国家振興策（VISION 2020）を掲げている。産業構造の転換を図り、サービス・知識産業が一層の成長を遂げることを目標としている。

その中で情報通信分野は優先度の高い重要事項として扱われており、特に 1996 年には、その具体策としてMSC（マルチメディア・スーパー・コリドール）計画を発表し、ハイテク産業の集積地としての次世代首都の建設を実現すべく構想を進めている。

マレーシアの人口とインターネット加入者の推移



マレーシアのインターネット普及推移

	1992 年	1993 年	1994 年	1995 年	1996 年	1997 年	1998 年	1999 年	2000 年 1 月	2000 年 3 月	2001 年 1 月	2001 年 9 月
人口（百万人）	19.0	19.6	20.1	20.7	21.2	21.7	22.2	22.7	23.3	23.4	23.5	23.7
インターネット加入者（百万人）	NA	NA	NA	0.014	0.064	0.205	0.405	0.668	1.659	1.842	2.009	2.372
年間成長率（%）	-	-	-	-	357.1	220.3	97.6	64.9	148.4	-	-	-
人口比率（%）	-	-	-	0.1	0.3	0.9	1.8	2.9	7.1	7.9	8.5	10.0

(a) ＭSC（マルチメディア・スーパー・コリドー）概要

マレーシアで1991年に掲げられたＶISION2020実現にむけての具体策の１つであり、情報通信産業を中心とする産業構造の高度化を目的とした計画である。

MSC 計画は、総工費 6000 億（約 2 兆円）を投じて、マレーシアにおいて建設中の新行政都市「プトラ・ジャヤ（Putrajaya）」（2005 年完成予定）と新インテリジェント都市「サイバー・ジャヤ（Cyberjava）」（1998 年一部完成）を中心に、首都クアラルンプールの南方から、新首都商業中心「クアラルンプール・シティ・センター（KLCC）」及び「クアラルンプール新国際空港（KLIA）」（98 年 6 月 30 日開港）を結ぶ東西 15km×南北 50km の地域（ほぼシンガポールの面積に相当）に 2.5GB から 10GB までの大容量・高速光ケーブルを施設して、世界的規模の情報通信企業や研究開発組織、通信サービスのヘビーユーザであるサービス産業やハイテク製造業（例えば半導体製造業など）を誘致し、21 世紀に向けている世界のマルチメディア拠点として発展させるという国家プロジェクトである。

「プトラ・ジャヤ（Putrajaya）」は、マレーシアの新電子行政都市であり、首都機能をすべて移転する予定がある。建設の予定は 2005 年に完成するが、99 年にはマハティール首相が「プトラ・ジャヤ」へ首相官邸を移転すると発表した。この「プトラ・ジャヤ」は、電子のリングによって、クアラルンプールと相互接続される。また、97 年 5月からマレーシア政府はMSC 計画の中核インテリジェント都市として「サイバー・ジャヤ（Cyberjava）」の開発・建設を進めている。

「サイバー・ジャヤ」は主とクアラルンプールの南方のハイテクゾーン、ＭSCの中央部に位置し、広さは約 750 平方キロである。「サイバー・ジャヤ」は、マルチメディア関連の事業、研究・開発の拠点となり、2020 年までに人口 24 万人、誘致企業 500 社を目標している。企業を誘致するだけでなく、マルチメディア大学や様々な研究開発機関も建設され、通信情報産業の重要拠点とする。

MSC で実現しようとしている具体的な計画事例として、以下 7つの項目が決められた。

① 電子政府 (Electronic Government)

② 多目的国民カード (National Multipurpose Card)

③ スマート学校 (Smart School)

④ 遠隔医療 (Telemedicine)

⑤ 研究開発拠点 (R&D Clusters)

⑥ 国境なきマーケッティング・センター (World-wide Manufacturing Webs)

⑦ 国際的遠隔製造業網 (Borderless Marketing Center)

マレーシアの情報通信産業関連政策

政策経緯	1991　VISION2020 公表 1996　MSC構想公表 1999　サイバー・ジャヤ開所
代表的面開発	マルチメディア・スーパー・コリドー
特徴	マルチメディア産業
面積	75,000ha
企業数	347 社（認可ベース）
研究技術者数	7 千人（全体）
生産額	－
地域の特徴	国主導の巨大開発と外資依存
ITへの取組の特徴	迅速な行政の対応 （インフラ、法制、人材育成）
競争力の源泉	マハティール首相の指導力とネットワーク 低廉なビジネスコスト 英語が通用
国土面積	328,000？
人口	22,000,000 人
一人あたりGDP（名目）	3,268 米ドル
インターネット普及率	8.0%

（平成 13 年）

(2) MSC（マルチメディア・スーパー・コリドー）とサイバー法

MSC 計画を実現させるために欠くことのできないものの 1つが、サイバー法の制備である。サイバー法の整備は重点課題として取り組まれてきており、アジア地域の中でも先頭を切って整備が進められている。MSC におけるソフトインフラ整備の一環として重要な要素となっているサイバー法については１９９７年、マレーシア議会により4つのサイバー法が制定された。それら

は、

① デジタル署名法（The Digital Signature Act 1997）
② 遠隔医療法（The Telemedicine Act 1997）
③ コンピュータ犯罪法（Computer Crimes Act 1997）
④ 1987年著作権法改正法（The Copyright (Amendment) Act 1997）

である。また、1998年7月には、

⑤ 通信・マルチメディア法案（The Communications and Multimedia Act 1998）

が議会を通過している。

(a) コンピュータ犯罪法（Computer Crimes Act 1997）

コンピュータ犯罪法は2000年6月1日に施行され、コンピュータの不正使用罪を規定している。この法律は、コンピュータのプログラム、データ、その他の情報を所有する者が、本来それらを所有する権限がないにも関わらず所有している場合は、推定規定によって対処しようとするものである。すなわち、その者が不正なアクセスで入手したとの推定について反証できないときは、不正アクセスが行われたと推定し、不正アクセス罪を適用することになる。また、法の適用範囲についても規定している。

以下に、刑事実体法の部分を抜粋、仮訳する。

第3条　コンピュータ・マテリアルに対する無許可アクセス

(1)以下の者は有罪である。

a. コンピュータ内にあるプログラム、もしくはデータに対するアクセス権を入手する意図でコンピュータに何らかの機能を実行させ、
b. 入手を意図したアクセスが無許可であり、かつ、
c. その者が、コンピュータに機能を実行させた時点において問題を認識していた場合。

(2)本条の犯罪を実行するものの意図が、以下のものに向けられている必要はない。

a. 特定のプログラムもしくはデータ

b. 特定の種類のプログラムもしくはデータ、または、

c. 特定のコンピュータ内にあるプログラムあるいはデータ

(3)本条の犯罪を実行し、有罪となった者は、50,000 リンギット以下の罰金刑、もしくは 5 年以下の拘禁刑に処し、または、これらを併科する。

第 4条　犯罪を実行する意図、または、他の犯罪を容易にするような無許可アクセス

(1)次のいずれかの意図で、第 3条に示す犯罪行為を実行した者は本条により有罪である。

a. 詐欺や不正行為を含む犯罪を実行する意図、または、刑法に規定された侵害を発生させるような意図、または、

b. 本人もしくは、その他の者がそのような犯罪を実行することを容易にする目的

(2)本条においては、本条で適用される犯罪行為が、無許可アクセスがなされたと同時であったか、もしくはその後の機会に実行されたかは重要ではない。

(3)本条の罪を実行して有罪となった者は、150,000 リンギット以下の罰金刑、もしくは 10 年以下の拘禁刑に処し、またはこれを併科する。

第 5条　コンピュータコンテンツの無許可改竄

(1)コンピュータコンテンツの無許可改ざんを発生させることになるだろうことを認識しながら、なんらかの行動を起こした者は有罪である。

(2)本条においては、問題となる行動が、以下のいずれかを目的としていないことは問題ではない。

a. 特定のプログラムもしくはデータ

b. 特定の種類のプログラムもしくはデータ、または、

c. 特定のコンピュータ内にあるプログラムもしくはデータ

(3)本条においては、無許可改ざんが恒久的なものか一時的なものか、または、恒久的なものとして意図されたものか一時的なものとして意図されたのかは重要ではない。

(4)本条の罪を実行して有罪となった者は、100,000 リンギットの罰金刑、もしくは 7 年以下の拘禁刑に処し、またはこれらを併科する。刑法に規定する侵害の結果を発生させる意図でその行為が行われた場合には、150,000 リンギットの罰金刑、もしくは 10 年以下の拘禁刑に処

し、またはこれらを併科する。

第6条　違法通信

(1)通信のための適法な権限を有する者以外の者に対し、番号、コード、パスワードやその他のコンピュータにアクセスするための手段を直接または間接に送信した者は有罪である。

(2)本条の罪を実行して有罪となった者は、25,000リンギットの罰金刑もしくは、3年以下の拘禁刑に処し、またはこれらを併科する。

第7条　教唆及び未遂は犯罪として処罰される

(1)本法に基づく犯罪行為の実行を教唆した者、または、その実行を試みたものは有罪であり、その犯罪行為について規定する処罰条項によって処罰される。

(2)本法に基づく犯罪行為の実行を準備する行為、または、その実行を容易にする行為を実行した者は有罪であり、その犯罪行為について規定する処罰条項によって処罰される。但し、科されるべき拘禁刑の期間は、それぞれの犯罪について規定する最長期間の 2 分の 1 以下とする。

第8条　推定

保管もしくは管理する権限のないコンピュータ内にあるプログラム、データその他の情報、または、そのようなコンピュータから検索したプログラム、データその他の情報を保管もしくは管理する者は、反対の事実が証明されない限り、当該プログラム、データもしくは情報に対する無許可アクセスを入手したものと推定する。

第9条には、本条約の適用範囲が記されている。英文を抜粋すると、

Territorial scope of offences under this Act

9. (1) The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question,

the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time.

(3) Any proceeding against any person under this section which would be a bar to subsequent proceedings against such person for the same offence if such offence was committed in Malaysia shall be a bar to further proceedings against him under any written law relating to the extradition of persons, in respect of the same offence outside Malaysia.

上記の記述からこの条約では、マレーシア国内の人間の犯行のみではなく、犯罪を実行した時点でコンピュータ、プログラム、データ等がマレーシアにある場合、どこの国に属する人間であろうと適用される。つまり、犯罪の原因がマレーシアにあろうと、犯罪の結果がマレーシアに起ころうとも、犯行をマレーシア国内、国外から実行したことに関わらず処罰対象になるということである。

(b) その他のハイテク関連分野についての法律

①デジタル署名法（The Digital Signature Act 1997）

1998 年 10 月 1 日施行されたデジタル署名法は、認証機関監督官の任命と、規制の最低限として、認証機関の免許制を義務づけている。本法は、認証機関の運営において、信頼性の基本的なレベルについて定める。すなわち、免許を欠く認証機関を無効にすることによって、署名の信頼性を損なうことのないようにするものである。規定には、免許の付与条件や、免許の取り消し、罰則、認証書発行申請などがある。

②遠隔医療法（The Telemedicine Act 1997）

遠隔医療法は、遠隔診断（telemedicine）とそれに関連する事項の実施にあたってのルールと国の監督体制について定める。特に、この法律は、遠隔診療行為を指定された医師によることを条件とする。また、マレーシア国外で登録されている医療関係者も遠隔診療を実施するための許可証を得ることにより、実施することが可能である。 まだ施行はされていない。

③著作権法改正法（The Copyright (Amendment) Act 1997）

1999 年 4 月 1日に施行された著作権法改正法は、MSC 計画の成功を支援する目的で、技術的進展に配慮した見直しが必要となったために、改正を行ったものである。改正法の保

護対象には、教育的著作物や娯楽作品のほか、本来、著作権の対象とならないコンピュータ情報などが含まれており、ネットワーク環境に配慮した著作物の保護がはかられている。その他CD等のコピー・プロテクション装置の解除行為を処罰する規定もおく。

④通信・マルチメディア法案（The Communications and Multimedia Act 1998）

1999年4月1日に施行された通信・マルチメディア法案は、マレーシアを、世界的に有数の通信とマルチメディアインフォメーション、コンテンツサービスの中心とするための法制であり、テレコミュニケーション、放送、コンピュータ産業の集中をまかなうことを目的に取締りをするフレームワークを提供するものである。つまり、既存の電気通信産業の効率向上と、マレーシアにおける新たな情報技術産業およびマルチメディアサービス産業の開発促進を目的とし、現行の電気通信法・放送法を簡素化し、双方向オンラインサービスの規定を設けた。マレーシアの通信とマルチメディアのための委員会は、新しい体制の唯一の取り締まり機関として1998年11月1日に設営された。法として認可された形だが、新しく規定されたフレームワークの基本の1つは、IT及びマルチメディアコンテンツ産業を含む様々な産業による自己統制である。

これまでみてきたように、マレーシアはマルチメディア・情報通信分野の高度化、ひいては外国資本の誘致のため、サイバー法の整備に力を注いでいる。時代の潮流を先取りした感のあるMSC計画であるが、国内経済は未だ安定を見ておらず、実現への道は険しいものであるという。

しかし、マレーシアはサイバー法の制定という部分に重要性を認めているようであり、

- 電子政府法案（Electronic Government Bill）
- データ保護法案（Data Protection Bill）

を準備中である。

マレーシアのサイバー法制定時系列

デジタル署名法 The Digital Signature Act 1997 恐らく、アジアで成立したはじめてのデジタル署名法。	1997 年成立 1998 年 10 月 1 日施行
著作権法改正 The Copyright (Amendment) Act 1997 1987 年の著作権法を改正する法律。日本の 97 年著作権法改正における公衆送信可能化権の導入と同等の改正。著作権情報管理や複製禁止回路の迂回等を非合法化する改正も含む（WIPO 著作権条約の実施等）。	1997 年成立 1999 年 4 月 1 日施行
コンピュータ犯罪法 The Computer Crimes Act 1997 不正アクセスの禁止等を規定	1997 年成立 2000 年 6 月 1 日施行
遠隔医療法 The Telemedicine Act 1997 AV 技術、通信技術を用いて遠隔地から医療行為を行うためのフレームワークを提供する法律。但し2000 年末現在未発効である。	1997 年成立 2000 年末現在未施行
通信・マルチメディア法 The Communications and Multimedia Act 1998	1998 年成立 1999 年 4 月 1 日施行
電子政府法案 Electronic Government Bill	準備中
データ保護法案 Data Protection Bill	準備中

(3) その他マレーシアのハイテク産業への取り組み

(a) MMU（Multi Media University）

マハティール首相が 1995 年に提唱した、ITを中心としたサービス・知識集約型産業を育成する計画には、高度な知識を有する技術者が不可欠であるとの認識のもと、その人材育成の中心が Multi Media University（MMU）である。

テレコム・マレーシア（過半数の資本を政府が保有）が、100%出資で設立した私立大学である。Cyberjaya キャンパスは1999年 7月にオープンしたが、1995年 10月にマレーシア初の民間大学としてマラッカに設立されたテレコム大学が、その前身であり、ここは MMU のマラッカ・キャンパスとなっている。

サイバー・ジャヤ・キャンパスには、Creative Multimedia 学部、Engineering 学部、Management 学部および Information Technology 学部の四学部があり、マラッカ・キャンパスには、Information Science & Technology 学部、Engineering 学部および Business & Law 学部の三学部がある。 学生は全体で、12，000名。大学院生も、Ph.D が 80名、M.Phil が 126名、M.Eng.が 62名、MBA が 264名。日・米・欧の民間企業が教授派遣、設備提供、講座開設などの協力を行っている。 教員は、600名で、それ以外に約 500名のスタッフがいる。 授業料は 11，000～1

2，000RM（約30万円～40万円）で工学部は13，000RMで少し高い。学生はほとんどが政府の奨学金（日本の育英資金に相当）を受領している。 授業は、三学期制（6月～8月、9月～12月、1月～4月）で、ここは他の国立大学とは異なり、学期間の休みはせいぜい二週間程度ということであり、学生も教員も結構忙しい。

すべて英語による授業が行われている。 サイバー・ジャヤ・キャンパスは新しいこともあり、広大な土地にゆったりと各施設が建っているという最高の環境で、学生は全員寮生活で、図書館も夜12時まで空いており、Internet利用による情報検索も可能となっている。

7. シンガポールにおけるハイテク犯罪対策

(1) シンガポールのIT政策とその成果

近年シンガポールにおいてIT産業が発展している要因は、ITが競争社会で勝ち残る為の重要なファクターになるという点に早くから気がついていたからである。1991年にはNational Information Technology Council (NITC) と National Computer Board (NCB)の指揮のもとNational Information Infrastructure (NII)プランをスタートさせる。予断であるが、シンガポールがNIIプランを始めたのはアメリカを始めとする諸外国よりもずいぶん前のことであった。そして、そのプランは順調に進行し、多くの外資系企業がシンガポールでのビジネスを展開し始めた。シンガポールはヨーロッパ諸国、中東諸国、インドとアジア諸国(中国、香港、台湾、韓国、日本)を結ぶための拠点として確固たる地位を築いていった。

この後、1990年代のIT推進計画である、The IT 2000 vision (IT 2000計画) を1992年に策定し、21世紀に向け、シンガポールのインテリジェントアイランド化を念頭に、(1)シンガポールのグローバルハブ化 (2)経済発展の推進 (3)個人の能力の増強 (4)社会の地域的、国際的リンク (5)生活品質の向上 を目指していった。1996年の時点で、IT部門は、シンガポールGDPの20%に当たる260億Sドル(約1兆8000億円) を寄与していた。この数字からも、シンガポール経済におけるIT部門の重要性とシンガポール政府の熱心なIT政策の成果を見ることが出来る。

IT2000計画を具体化するものとして、1996年に提唱されたのがシンガポールワン計画である。同計画は、国内に高速広帯域ネットワークを構築し、オフィスから家庭までマルチメディアサービスの提供の実現を目指すものであった。そして、今日では高速広帯域ネットワークと洗

練された市場を背景に、シンガポールワンは、マルチメディアサービスを研究開発、商用化するための理想的な環境を提供していると言える。

最近の事例として 2000 年から 2010 年の間の計画としての、ICT21 基本計画がある。これは、e ワールドの新たな時代に向け、ンガポールにおける情報通信技術（ICT-Information and Communications Technology）開発を促進するための基本計画である。この計画の中でシンガポールは 2010 年までにグローバル情報通信技術（ICT）の首都になることを目標としており、(1)経済繁栄のキーとなる ICT 部門の設立 (2)知識集約型経済を拡大する共通プラットホームとしての ICT 活用 (3)将来の情報化社会における国民生活の品質向上をターゲットにしている。

ここで、アジア圏内のインターネット普及率をみてみたい。2000 年末調査の 1 位がオーストラリア（38.3%）、2 位が台湾（37.6%）、3 位が韓国（36.8%）。以下シンガポール（34.0%）、香港（31.7%）、ニュージーランド（30.6%）、日本（23.4%）、マレーシア（14.0%）、タイ（2.3%）、中国（1.5%）と続いている。中国・インドは約 10 億人の人口を持つため、インターネット人口が伸びても普及率の上昇にはなかなかつながらず、インドに至っては普及率はわずか 0.3%だ。アジアをもっと狭めて ASEAN 圏内で見るといかにシンガポールが IT 分野で進んでいるかという事が分かる。2000 年初頭の数字である為、上記のものと多少ばらつきがあるが、シンガポール(29.8%)、マレーシア（15.9%）、フィリピン（2.6%）、タイ（1.9%）、インドネシア（0.7%）と、一歩も二歩も抜きんでている。

(2) Computer Misuse Act(コンピュータ不正使用禁止法) 改訂版

NII プラン(1991 年)、IT 2000 計画(1992 年) の実施に伴い、IT 産業が発達していく過程で既成のハイテク犯罪に対する法律への疑問点が数々浮かび上がってきた。そのため、法整備の必要性が問われるようになり、1993 年に最初の The Computer Misuse Act(コンピュータ不正使用禁止法)が制定され、ハッキング、ウィルスの散布、情報の窃盗行為などは犯罪として規定された。また、この法律には、ハイテク犯罪の被害者を保護する内容も含まれていた。そして、5 年後の 1998 年の 7 月 1 日にはその改訂版が議会で審議され始め、同月の 28 日に承認、8 月 1 日に施行された。

Computer Misuse Act(コンピュータ不正使用禁止法) 改訂版は第 1 部、第 2 部、第 3 部に分かれており、全 16 条からなる。その中から重要と思われる部分を抜粋して和訳した。

第 3 条 Unauthorised access to computer material

(コンピュータ・マテリアルに対する不正アクセス)

コンピュータ内のプログラムもしくはデータに無権限でアクセスを実行した者は、有罪であり、5,000 ドル以下の罰金刑もしくは 2 年以下の拘禁刑に処され、または、これらを併科する。再犯またはそれ以上の累犯の場合には、10,000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑、または、これらを併科される。

また、不正アクセス行為の結果として何らかの損害が生じた場合、その犯罪行為を実行した者は、50,000 ドル以下の罰金刑もしくは 7 年以下の拘禁刑、または、これらを併科される。

第 4 条 Access with intent to commit or facilitate commission of offence

(違法行為を意図したアクセス)

財産権を侵害する犯罪、詐欺罪、背任罪もしくは身体の危険を生じさせるような犯罪行為の実行を意図して、コンピュータ内のプログラムもしくはデータへのアクセスを実行した者は、有罪であり、2 年以上の拘禁刑に処される。(刑期は最長で 10 年、また、罰金は最大で 50,000 ドルであるが、これらが併科される場合もあり得る。)

また、この条に於いて、違法行為実行者の被害を与えたコンピュータへのアクセス権限の有無は重要ではないと定められている。

第 5 条 Unauthorized modification of computer material

(コンピュータ・マテリアルの不正修正)

コンピュータのコンテンツを無権限で修正した者は、有罪となり、10,000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑に処され、または、これらを併科される。再犯またはそれ以上の累犯の場合、20,000 ドル以下の罰金刑もしくは 5 年以下の拘禁刑、または、これらを併科される。

修正の結果として何らかの損害が生じた場合には、修正行為を実行した者は、50,000 ドル以下の罰金刑もしくは 7 年以下の拘禁刑となり、これらを併科される場合もある。

第 6 条 Unauthorized use or interception of computer service

(コンピュータ・サービスの不正使用または傍受)

コンピュータ・サービスの不正使用または傍受を行った者は有罪であり、10,000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑に処され、または、これらを併科される。再犯またはそれ以上の累犯の場合には、20,000 ドル以下の罰金刑もしくは 5 年以下の拘禁刑、または、これらを併科される。

これらの行為の結果として何らかの損害が生じた場合には、実行者は、50,000 ドル以下の罰金刑もしくは 7 年以下の拘禁刑、または、これらを併科される。

第 7 条 Unauthorized obstruction of use of computer

コンピュータ使用の不正妨害

不正、不法にコンピュータの利用を阻害した者、もしくは、妨害した者、コンピュータ内に記憶されたプログラムもしくはデータへのアクセスを妨害した者は有罪であり、10,000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑、これらを併科される。再犯またはそれ以上の累犯の場合には、20,000 ドル以下の罰金刑もしくは 5 年以下の拘禁刑、または、これらを併科される。

これらの行為の結果として何らかの損害が生じた場合には、実行者は、50,000 ドル以下の罰金刑もしくは 7 年以下の拘禁刑、または、これらを併科される。

第 8 条 Unauthorized disclosure of access code

アクセス・コードの不正開示について述べられており、不正に、パスワードまたはアクセス・コード、その他、コンピュータ内に保持されたプログラムもしくはデータへのアクセスを得るための手段を開示した者は、その行為を、(a)不正の利益を得るために、(b)違法な目的のために、(c)他人に対し違法に損失を生じさせることになるだろうということを知りながら、実行した場合には、有罪である。

有罪となった場合、10,000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑、または、これらを併科される。再犯またはそれ以上の累犯の場合には、20,000 ドル以下の罰金刑もしくは 5 年以下の拘禁刑、または、これらを併科される。

第 9 条 Enhanced punishment for offences involving protected computers

(保護されているコンピュータに対する違法行為への加重処罰)

保護されているコンピュータの定義とは、(a)シンガポールの保安、防衛もしくは国際関係、(b)刑法の執行に関連する機密、(c)通信基盤、銀行及び信用供与、公共施設、公共運送もしくは公開鍵暗号基盤などに関連する情報を有しているコンピュータである。そして、この類のコンピュータに不正行為を行ったものは100,000 ドル以下の罰金刑もしくは20年以下の拘禁刑、または、これらを併科される。

第 11 条 Territorial scope of offences under this Act

(法律の適用範囲)

この法律は、(a)当該違法行為を犯した者の国籍または市民権を問わず、シンガポール内外のすべての者に対して有効であり、(b)違法行為がシンガポールの外で実行された場合でも、それがシンガポールの中で実行されたのと同様に取り扱われる。

また、当該犯罪行為が行われる以前の重要な時点に、(a)容疑者がシンガポール内にいた場合、または、(b)コンピュータ、プログラムもしくはデータがシンガポール内にあった場合でも同じようにこの法が適用される。

第 12 条 Jurisdiction of Courts

(裁判所が有する権利)

地方裁判所と簡易裁判所は、この中で定められているすべての犯罪行為を、この法の下で裁く権利を有し、刑事訴訟法 第 68 章)内に反対の条項が存在する場合であっても、それに制限されることはない。

第 13 条 Order for payment of compensation

(賠償金支払命令)

裁判所は有罪判決を宣告する前に違法行為によってコンピュータ、プログラムもしくはデータに損害が生じた場合の損害賠償金を支払うよう、被告に命ずることができる。

第 14 条 Saving for investigations by police and law enforcement officers

この法律は警察官及び法曹家たちによる捜査を妨げる物ではなく、助長するものである。

第 15 条 Power of police officer to access computer and data

(コンピュータ及びデータへアクセスする警察官の権限)

調査権限を得た警察官は、調査のためであれば、対象のコンピュータ、データにアクセス可能である。警察官の調査依頼を拒否または、調査を妨害した者は 10.000 ドル以下の罰金刑もしくは 3 年以下の拘禁刑、または、これらを併科される。

第 16 条 Arrest by police without warrant

(警察官による無令状逮捕)

警察官は、この法の下、違法行為を実行したと思われる容疑者を、令状なしに逮捕することができる。

⑶ ハイテク犯罪への対抗策

シンガポール政府は、ハイテク犯罪に対抗する為に、the Computer Crime Branch と、Computer Forensic Branch と呼ばれる 2 つの機関を設立し、この法の下ハイテク犯罪を厳しく取り締まっている。Computer Misuse Act 第 16 条で、警察官が令状なしに容疑者を逮捕できる特権を規定していることがこのことを如実に表しているといえる。1 つシンガポールのハイテク犯罪に対する厳しい姿勢を示す判例を挙げておく。17 歳の学生が Swiftech の Automation's computer system をハッキングし、システムを不正に変更するという事件があった。当初、地方裁判所の判決では、この少年に対して、30 ヶ月の執行猶予が与えられただけであった。しかし、この判決は上級裁判所でひっくり返される。そこでの裁判官の論旨は、こうである。”ハッキングに代表されるハイテク犯罪は概ね家から行われる。なのに、普通の少年犯罪と同じようにこの少年を家で謹慎させる事を処罰とするのはおかしい”。結局この少年は、4 ヶ月の拘禁刑に処された。

ハイテク犯罪者を検挙する事は容易ではない。その理由はコンピュータを使えばいくら離れた場所からでも違法行為を実行できるからである。厳しい法律を持つシンガポールにおいてもハイテク犯罪は減るどころか増加の傾向にあるが(表参照)、シンガポールは Computer Misuse Act 第 11 条を規定することによって国外からの違法行為に対しても厳しい対応を行っている。

2000 年の 7 月に、Singapore research and development institute のサーバに侵入した

インドネシア人の少年が逮捕されたが、この少年がハッキングを行ったのは、この年の3月から4月にかけて留学先のオーストラリアからであった。この少年はターゲットとなったサーバが脆弱であるという事をインターネットのチャットルームを通して知ったと警察は話している。少年は、その後、英語と数学の勉強の為にシンガポールに移って来てからも、ハッキングを続けていたが、前述した the Computer Crime Branch によって逮捕される事となった。裁判の結果この少年の保釈の為に払われた金額は 10,000 シンガポール ドル(日本円で約 158 万円)であった。(ちなみに日本国の不正アクセス対策法では、不正アクセス行為に対しては懲役 1 年以下もしくは 50 万円以下の罰金、不正アクセス助長行為に対して 30 万円以下の罰金である。)

しかし、厳しい法律が存在するだけでは、外国からのハッキングに十分な対応は出来ない。外国からシンガポール内のコンピュータがハッキングされた時に、その犯人を検挙する為に重要になってくるのはその犯人が住む国の国家警察や調査機関との連携である。例を挙げると、2000 年 4 月に出現し、世界中で 100 億 US ドル以上の損失を出した"I Love You"ウィルスをばらまいた容疑者の検挙は、アメリカの FBI と、FBI と親密な関係を保持しているフィリピンの国家調査機関との連携によって実現した。しかし、この当時フィリピンにはハイテク犯罪を取り締まる為の法整備が成されておらず、容疑者は罪に問われなかった。

表　　シンガポールハイテク犯罪の数

Year	報告された件数
1993-1994	1
1995	3
1996	14
1997	39
1998	116
1999	185
2000(1 月-7 月)	127

8. 欧州評議会におけるハイテク犯罪対策

(1) ハイテク犯罪への取り組み

欧州評議会によるコンピュータ犯罪に対する取り組みは、1980 年代の終わりに始まった。それまでは欧州評議会各国は個別に対応していたが、ボーダレスなコンピュータ犯罪が増加

するにつれ、共通の国際的文書策定や共同調査などの必要性認識し、共同でコンピュータ犯罪対策に取り組むようになった。その動きは 1989 年のコンピュータ犯罪に関する勧告 No R(89)9（参考 URL8 番参照）と、1995 年の情報技術に関連する刑事手続法上の諸問題に関する勧告 No R(95)13（参考 URL 9･15 番参照）により顕著となった。それらの勧告をもとに、欧州評議会は、情報技術に関する法案策定についての諸問題を検討すべく、世界的なコンピュータ法の権威として知られるアムステルダム自由大学 Kaspersen 教授に調査を依頼した。その結果教授は、実体法的な問題だけではなく、刑事的手続きと国際的機構についてもカバーする内容となるのが望ましいという内容の報告を行った。

kaspersen 教授の調査報告を受けて、1996 年 11 月に、欧州犯罪問題委員会（CDPC = The European Committee on Crime Problems）は、コンピュータ犯罪対策とそれに付随した国際的文書作成を目的とする専門委員会を設置する決定 CDPC/103/211196 に合意した。

その合意内容のもと、CDPC の決定を受けた閣僚委員会が、第 583 回の閣僚代表者会合（1997 年 2 月 4 日開催）で採択された CM/Del/Dec/(97)583（参考 URL11 番参照）によって正式に、「サイバー・スペースにおける犯罪に関する専門家委員会(PC-CY = The Committee of Experts on Crime in Cyber-space)」を設置した。

(2) 条約制定の経緯

国際的な法律文書策定を目的として設置された PC-CY は、

① サイバー・スペース犯罪の実態・定義
② 国際協力の際に必要となる刑法上の事項
③ 国境を越えた強制力の適用可能性
④ コンピュータ犯罪における裁判管轄権の問題
⑤ サイバー・スペース犯罪の捜査における国際協力問題

の 5 つの調査事項を重点に置きつつ、1997 年から 2001 年まで本会合 10 回、条約草案会合を 15 回行った。当初は 1999 年 12 月 31 日までにその作業を終えるはずであったが、条約草案に問題があり、その期限までに折衝を完全に終えることができなかった。そこで、閣僚代表者会議の決定 CM/Del/Dec(99)679 により、その調査期限が 2000 年 12 月 31 日まで延長されることになった。

欧州各国の司法相は、2 度にわたって PC-CY の調査に対する支持を表明した。一つは第 21 回欧州司法閣僚会議（プラハ、1997 年 6 月）で採択された決議 No.1 である。その内容は、

サイバー犯罪に関して効果的な捜査を可能にするために、各国の国内刑法の条項を相互に近いものにして、サイバー犯罪に関してCDPCが行っている作業を支持するよう閣僚委員会に対して勧告するというものであった。もう一つは第23回欧州司法閣僚会議（ロンドン、2000年6月）において採択された決議No.3である。その内容は2つあり、1つは可能な限り多数の国家が条約加盟国になることができるよう適切な解決策を見出すために、折衝当事国が努力を尽くすように促す内容であった。もう1つは、早急にサイバー犯罪に対して立ち向かうことを特定する要件として考慮された国際協力システムの必要性を認めるものであった。

延長した調査期限終了に伴い、会合に参加した専門家達は、議員会議の意見を考慮に入れた上で説明用覚書草案を確定した。そして、条約草案の見直しを計るためにCDPCの後援を受け、会合を重ねた。総会は、2000年10月閣僚委員会から条約草案について意見を提出するよう要請を受け、2001年4月に開催された本会議の第2部において条約草案を採択した。改訂された条約草案及び説明用覚書草案は、2001年6月の第50回CDPC本会議において承認された。そして、2001年11月8日、閣僚委員会において正式に採択され、同月23日、ブダペストにおいて開催された署名式にて署名された（2002年1月末現在の署名国は、G7各国、南アを含む32か国）。今後加盟各国が批准し、発効する。

年表 ------欧州評議会のサイバー犯罪に対する取り組みから条約調印まで-----

1989 年 9 月	コンピュータ犯罪に関する勧告 No R(89)9
1995 年 9 月	情報技術に関連する刑事手続法上の諸問題に関する勧告 No R(95)13
1996 年 11 月	CDPC がサイバー犯罪を取り扱う専門委員会を設置する決定 CDPC/103/211196 に合意
1997 年 2 月	第 583 回閣僚代表者会合で採択した CM/Del/Dec/(97)583 により「サイバー・スペースの犯罪に関する専門家委員会(PC-CY)」を設置
1997 年 6 月	第 21 回欧州司法閣僚会議（プラハ）で CDPC の作業を支援するために、各国の法律条項を近くするよう閣僚委員会に促す。
1997 年～2000 年	PC-CY はこの間に本会合 10 回、条約草案会合を 15 回行う。
1999 年 5 月	EU（欧州連合）が PC-CY の作業に対する支持を共同見解を通じて表明
2000 年 4 月	サイバー犯罪条約草案公開
2000 年 6 月	第 23 回欧州司法閣僚会議（ロンドン）にてサイバー犯罪に関する国際協力システムの必要性を認める決議を出す。同時に、多くの国が条約に加盟できるように PC-CY に努力するよう促す。
2001 年 4 月	欧州閣僚委員会にてサイバー犯罪条約草案採択
2001 年 6 月	CDPC にて草案が最終条約案として採択される。
2001 年 11 月 8 日	閣僚委員会にて正式に条約として採択される。
2001 年 11 月 23 日	ブタペスト開かれた国際会議にて正式に日本含む 32 カ国が署名

(3) サイバー犯罪条約の概要

サイバー犯罪条約は全部で

1 章 用語の使用-----用語の定義（第 1 条）

2 章 国内で採られるべき措置-----刑事実体法、手続法規、管轄権（第 2 条～第 22 条）

3 章 国際協力-----一般原則、特別規定（第 23 条～第 35 条）

4 章 最終条項-----条約の発効、改正、留保などに関する規定（第 35 条～第 48 条）

の 4 章で構成されている。ここで、条約の核を成し、重要であるのはサイバー犯罪の定義・手続法規を記している 2 章と、国際協力について定めた 3 章であるので、主にこの 2 つの概要を説明する。

(a) 2章 ：国内レベルで採られるべき措置

第 1 節-----刑事実体法（第 2 条～第 13 条）

第 1 節は、4 つに分類されたサイバー犯罪の定義と制裁条項などで構成され、さらに、それぞれについての詳細事項を規定している。Ⅳで詳しく後述するので、ここでの説明は割愛させて頂く。

第 2 節------手続条項（第 14 条～第 21 条）

第 1 款　共通規定

加盟各国は、この条約で定められた権限および手続きを設ける上で必要となる立法及びその他の措置を採用する。（第 14 条、第 15 条）

第 2 款　コンピュータ・データの応急保全

コンピュータ・データ*1 及びトラフィック・データ*2 の滅失・改変の恐れがあるとする根拠があった場合にその応急保全をデータの保有者に命令する。また、そのデータの保有者に対しデータの完全性を維持させ、必要とあるならば開示させる。

データを保有するサービス・プロバイダが複数であっても、データの応急保全を利用できる。また、捜査機関等が、データを伝送したサービス・プロバイダ及び経路を特定するためにトラフィック・データの応急開示を確保する。（第 16 条、第 17 条）

*1------第 1 章の用語の定義では、「コンピュータ・システムに機能を実行させるのに適したプログラムを含めて、コンピュータ・システムで処理するのに適した形式による、事実、情報又は概念の表現を意味する」とある。

*2------第 1 章の用語の定義では、「コンピュータ・システムという手段による通信に関連するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ・システムによって生成され、その通信の発信地、受信地、経路、時刻、日付、サイズ、持続時間又はその背後にあるサービスのタイプを示すものを意味する」とある。

第 3 款　提出命令

自国領土内の該当者に対するコンピュータ・データの提出、また、該当サービス・プロバイダに対する加入者情報の提出を命令することができる。（第 18 条）

加入者情報の定義----サービス・プロバイダによって保持され、コンピュータ・データ形式又はその他の形式で含まれるあらゆる情報。その情報は、サービス利用者に関連するものである。

また、その加入者情報によって

① 通信サービスのタイプ、そのために用 いられる技術設備及びサービスの期間

② 利用者の身元、住所、電話番号その他のアクセス番号、請求及び支払に関する情報

③ サービスを利用できる通信機器の設置場所に関するその他の情報を確定できるもの

を意味している。

第 4 款 コンピュータ・データの捜索及び押収

コンピュータ・データ及びその記憶媒体を捜索・押収する権限を締約国の然るべき権限のある捜査機関は付与される。同時に該当データの複製及び保持、消去する権限も付与される。また、上記の手段を実行できる知識者や専門家に対し必要な情報を提供させる権限を有する。（第 19 条）

第 5 款 コンピュータ・データのリアルタイム収集

締約国はトラフィック・データまたは通信のコンテントデータ*3 をリアルタイムで収集・記録する権限を有する。また、サービス・プロバイダ*4 に対しても同様の協力・援助をさせる権限も付与される。サービス・プロバイダはこの権限が行使されていることに関しての機密保持を義務付けられる。（第 20 条、第 21 条）

*3----原文では、「コンピュータ・システムによって伝送される特定の通信と関連するコンテントデータ」と記してある。通信の中身に関するデータのことを表している。

*4----第 1 章の用語の定義では、「サービス・プロバイダとは①そのサービスの利用者に対してコンピュータ・システムという手段によって通信をする能力を提供する公的な主体又は民間の主体、及び②その他、そのような通信サービスに代わってもしくはそのようなサービスの利用者に代わって、コンピュータ・データを処理又は保存するその他の主体を意味する」となっている。つまりは、プロバイダ（ISP）だけでなく、メーリングリストや web サイトの主宰者などもこれに含まれることになる。

第 3 節-----管轄権（第 22 条）

各締約国は、犯罪行為が当該締約国の国民により自国領土内・国旗を掲揚した船舶内・登録さ

れた飛行機内にて起きた場合管轄権を有する。また、当該締約国の国民がその裁判権の及ばない地域で犯罪行為を起こしても、締約国の法律で処罰可能にする。2 カ国以上の締約国が管轄権を主張する場合、関係する締約国は管轄権について協議しなければ成らない。

(b) 3章 ：国際協力

第 1 節----一般原則 第 23 条～第 28 条）

第 1 款 国際協力に関する一般原則

各締約国は、コンピュータ犯罪に関する犯罪捜査及び刑事手続、または証拠の収集について、可能な限り広い範囲で相互協力しなければならない。 第 23 条）

第 2 款 引渡に関する原則

犯罪者の引渡は、各締約国間の双方の法律で、本条約で規定したコンピュータ犯罪の刑期が 1 年以上の自由刑より重い場合に適用される。各締約国はこの条件を現存する全ての引渡に関する条約に含めなければならない。また、請求を受けた締約国が引渡を拒絶した場合、自国 (請求を受けた国）の刑事訴追機関に事件を捜査させ、請求を行った締約国の求めに応じて報告を行わなければならない。 第 24 条）

第 3 款 相互援助に関する一般原則

各締約国はコンピュータ犯罪に関する犯罪捜査・刑事手続と証拠の収集について、可能な限り広い範囲で協力しなければならない。緊急の際は、要請を受けた加盟国からファックス又は電子メールなどの応急用通信手段によって、 必要に応じて、暗号化の使用も含め）相互援助の要請をすることができる。要請を受けた締約国は、このような応急用の通信手段の全てを受領し、応答しなければならない。また、他の締約国のコンピュータ犯罪捜査に有用であると判断した場合に、他の締約国の要請がなくとも、自発的に自国内捜査で入手したコンピュータ犯罪情報を送付することができる。 第 25 条、第 26 条）

第 4款 適用される国際協定がない場合の相互援助の要請に関する手続

相互援助の要請をする締約国と要請を受ける締約国間に、相互の法律に基づく相互援助協定がなかった場合にこの手続きが適用される。その場合、締約国は

① 窓口となる機関の設立を欧州評議会へ届け出る。

② 基本的に要請をした締約国の指定する手続きで相互援助要請は実施される。

③ 要請を受けた締約国は、財政に関する犯罪、政治的犯罪、またはその相互援助を実行することが自国の主権を損なうと判断した場合は要請を拒絶できる。また、延期の権利も保有する。

④ 要請を受けた締約国が拒絶・延期を行う前段階で、もし要請が部分的に認められるのであれば、要請をした締約国と協議を行い、その条件等を判断しなければならない。

⑤ 緊急時には各締約国の司法機関同士、または国際刑事警察機構（Interpol）を通じて要請・連絡を行える。

⑥ 要請を受けた締約国は、要請をした締約国が機密を保持し、また犯罪捜査または刑事手続き以外に使用しないことを条件に情報・資料を提供できる。（第 27 条、第 28 条）

第 2 節-----特別規定（第 29 条～第 35 条）

第 1款 仮措置に関する相互援助

各締約国は、他の締約国内にある押収や開示の必要があるコンピュータ・データの応急保全を要請することができる。要請を受けた締約国は

① その行為が犯罪でなかったとしても（要請を受けた締約国の法律では）直ちに応急保全の措置を取らなければ成らない。

② 要請が財政に関する犯罪、政治的犯罪に関するもの、もしくは自国の主権を損なうと判断した場合は要請を拒絶できる。

③ 要請に応えた場合、60 日を下らない期間、コンピュータ・データの保全を維持しなければならない。また、要請を受領した後、その要請に関する決定がなされるまでの間はそのデータを保全しなければならない。

また、上記の応急保全要請を行う過程で、他国のサービス・プロバイダがトラフィック・データに関与していた場合、要請を受けた締約国は要請をした締約国に対してサービス・プロバイダ及び経路を特定するための十分なトラフィック・データを応急的に開示しなければならない。この場合でも、要請を受けた締約国は、要請が財政に関する犯罪、政治的犯罪に関するもの、もしくは自国の主権を損なうと判断した場合は要請を拒絶できる。（第 29 条、第 30 条）

第 2 款 捜査権限に関する相互援助

各締約国は、必要に応じて他の締約国内にあるコンピュータ・データの捜索や押収、開示を要請することができる。

また、他の締約国から権限を得なくても、その締約国の適法な権限を持つ者の同意が得られれば、コンピュータ・データにアクセスし受領することができる。

各締約国はトラフィック・データ及びコンテントデータのリアルタイム収集に関してお互いに相互援助しなければならない。（第 31 条～第 34 条）

第 3 款　24/7 ネットワーク

各締約国は、犯罪捜査又は刑事手続、証拠の収集などの援助を即時に提供するために、週 7 日間・24 時間ベースで利用可能な連絡先を設けなければならない。この援助内容は、技術的な助言を提供することやデータを保全すること並びに証拠を収集し、法情報を供与し、容疑者の所在を特定することなどを促進するものとし、国内法及び慣行にて許容されている場合はそれらを直接実施することを含むものにしなければならない。（第 35 条）

⑷ 量刑・犯罪行為の定義

サイバー犯罪条約によると、第 2 章第 1 節で量刑と犯罪行為の定義づけを行っている。ここでは、コンピュータ犯罪は大きく 4 つに定義し、最後の第五款では犯罪の付随責任と制裁について触れている。特に現存する各国のコンピュータ犯罪法における定義と比べて目新しいものはないが、コンピュータ犯罪を取り締まる法律を制定していない国には指針となる。

第 1 款　コンピュータ・データ及びシステムの機密性、完全性及び可用性を侵害する犯罪行為

① 違法アクセス

不正なアクセスをコンピュータ・システムに対して行うこと。（第 2 条）

② 違法傍受

コンピュータ間の非公開のデータ通信を盗聴・傍受すること。（第 3 条）

③ データ妨害

不正にコンピュータ・データを改変、破壊すること。（第 4 条）

④ システム妨害

データ改変、破壊によりコンピュータ・システムの機能に障害を起こさせること。

第 5 条）

⑤ 機器の乱用・不正使用

①から④までの行為を目的とした製品（プログラム含む）を配布、販売、保有すること。 第 6 条）

第 2 款 コンピュータ関連犯罪

① コンピュータ関連偽造

法的に正しいと分かるものを、偽り悪用することを目的として改変・入力すること。（コンピュータによる公文書偽造等） 第 7 条）

② コンピュータ関連詐欺

経済上の利益を得る目的で、不正にデータの改変やシステムに障害を起こさせ、他人に損失を与えること。 銀行オンラインシステムに対するアタック行為など、相手に経済的ダメージを与えるもの）第 8 条）

第 3 款 コンテント関連犯罪

① 児童ポルノグラフィ関連犯罪

コンピュータ・システムを通じて児童ポルノを製造・提供・保有すること 第 9 条）

＊ 児童ポルノの定義-----あからさまな性行為を行っている未成年もしくは未成年に見える人物、もしくは未成年があからさまに性行為を行っているように表現する画像等。

＊ 未成年者の定義------原則として 18 歳未満だが、国によって独自の制限を設けることができる。ただし16 歳未満は認められない。

第 4 款 著作権及び関連諸権利の侵害に関連する犯罪

著作権及び関連諸権利の侵害に関連する犯罪-----パリ条約、ローマ条約、WIPO によって定義された著作権の侵害行為を、故意にコンピュータ・システムによって行うこと。

＊ パリ条約-----工業所有権の国際保護に関する同盟条約

＊ ローマ条約-----実演家、レコード製作者及び放送機関の保護に関する国際条約

＊ WIPO-----世界知的所有権機関(WIPO :World Intellectual Property Organization)

第 5 款 付随的責任及び制裁

① 未遂及び幇助又は教唆

第 2 条ないし第 10 条により設けられた犯罪行為の幇助または教唆を意図的に実行すること。第 3 条、第 5 条、第 7 条～第 9 条の未遂行為。（第 11 条）

② 企業責任

企業内において、ある一定の権限の与えられた人物が起こしたこの条約で設けられた犯罪行為に対するその企業の責任を問う。（第 12 条）

③ 制裁及び措置

各締約国は、サイバー犯罪条約にて定義された犯罪に対して、犯罪の重さに応じた抑止効果のある量刑を課す。なお、説明用覚書によれば、加盟国は既存の国内法システムと互換性が取れるようにある程度の裁量権を持って量刑を形成することができる。（第 13 条）

⑸ 各国の対応

現時点では署名したほとんどの国がサイバー犯罪条約に自国の法律をどのように適応させようとしているかは、検討中もしくは表明されていない。ただし、いくつかの国の政府の発表する公文書等で対応を（正式にではないが）記述している文書等が存在する。それらの文書を参考に、署名各国の対応を表に示す。不明は全く対応に関する情報が得られなかったもの。既存の法律が存在すると確認できた国は、何かしらの対応策を政府内で決定してからサイバー犯罪条約に署名していると考えられるので、検討中とした。

	既存の法律解釈で対応	法律改正で対応	新規法律作成	検討中	不明
アルバニア					○
アルメニア					○
オーストリア					○
ベルギー					○
ブルガリア					○
クロアチア			○		
キプロス					○
エストニア			○*1（2002 年 3 月新しい刑法が施行予定）		
フィンランド					○
フランス				○	
ドイツ				○	
ギリシャ					○
ハンガリー					○
アイスランド					○
イタリア				○	
マルタ					○
モルドバ					○
オランダ					○
ノルウェー					○
ポーランド		○*2			
ポルトガル				○	
ルーマニア					○
スペイン				○	
スウェーデン				○	
スイス				○	
マケドニア					○
ウクライナ					○
イギリス				○	
カナダ	△*3			○	
日本				○	
南アフリカ					○
アメリカ	○*4				

*1-----2002 年 3 月新しい刑法が施行予定。

（Country Reports: the situation of Cyber Crime in Various Countries

http://www.stopcybercrime.net/6_1.php 参照）

*2-----参考文書には名言はされてないが、既存の法律を改正する必要性があると記してある。

ただし、ポーランド政府公式の文書の可能性はほぼないので正確ではない。

（Computer Crime in Poland, Andrezej Adamski

http://www.law.uni.torun.pl/KOMP-LEX/Computer_crime_in_Poland.pdf 参照）

*3-----Anti-Terrorism Act という法令が、サイバー犯罪条約に対応したものであるとも受け取れる文章が参考文書にある。

（Anti-Terrorism Act Receives Royal Assent

http://canada.justice.gc.ca/en/news/nr/2001/doc_28215.html 参照）

*4-----以下のサイトに示された Q&A を参照する限りは現行法で対応可能との旨が記してある。

（Frequently Asked Question and Answers About the Council of Europe convention on cyber crime http://www.usdoj.gov/criminal/cybercrime/newCOEFAQs.html 参照）

第 3章　不正アクセス行為の傾向と手口

1. 不正アクセス行為の傾向

ここ数年、有名アプリケーションにセキュリティホールが発見されると、そのセキュリティホールを利用して感染活動を行うワームが作成され、インターネットに広まるという例が後を絶たない。著名な DNS サーバ・アプリケーションの BIND に発見されたセキュリティホールを利用した「lion Worm」、Solaris のデーモンプログラムとMicrosoft 社の IIS サーバに見つかったセキュリティホールを利用して感染する「sadmind/IIS Worm」、Microsoft 社の IIS サーバ、Internet Explorer に見つかったセキュリティホールを利用して感染する「Nimda Worm」というように、近年枚挙に暇がないほどワームが流行している。また、ウィルスも同様に「love You」ウィルスに始まり、「My Party」にいたるまで非常に多くのウィルスが蔓延している。そのため、「ワーム」そして「ウィルス」を不正アクセスの傾向としてとりあげる。

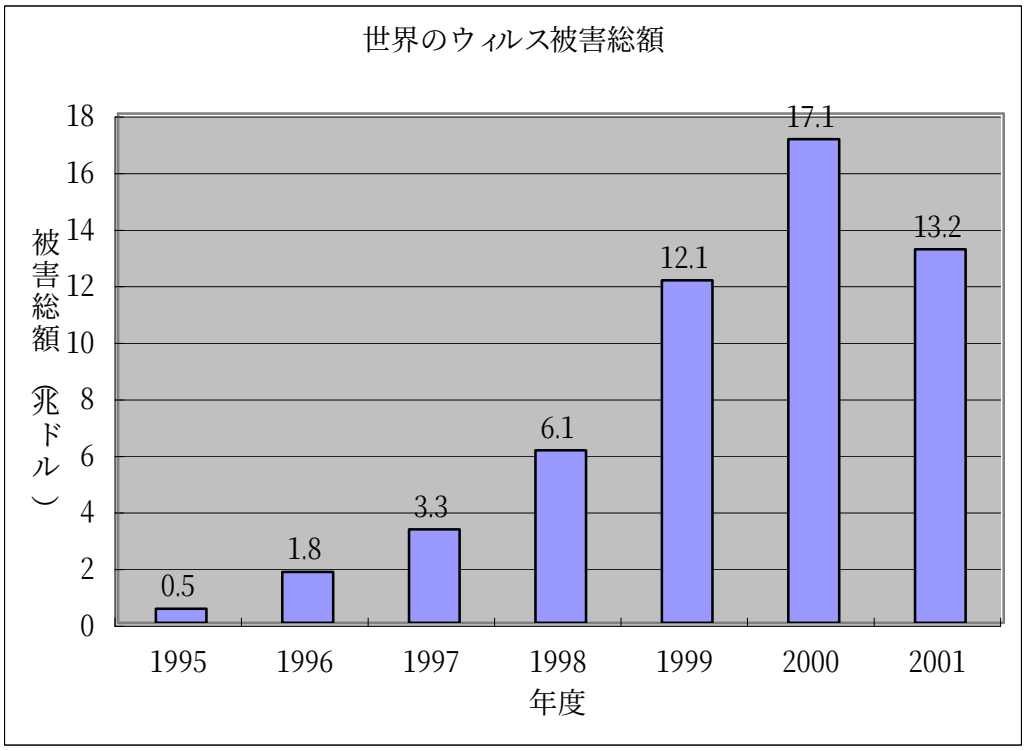
増加の一途をたどる「Web サイトの改ざん」にも注目し、また同様に Web サイトに関連した問題として最近騒がれるようになった、Web サーバ上で動作する独自開発アプリケーションのセキュリティホールにより、個人情報等が漏洩してしまう問題について取り上げる。さらに、攻撃されるために故意に脆弱性を持ったまま設置されている、ハニーポットに対して行われた攻撃の記録から、現実に行われている攻撃の傾向を探る。

(1) ワームとウィルス

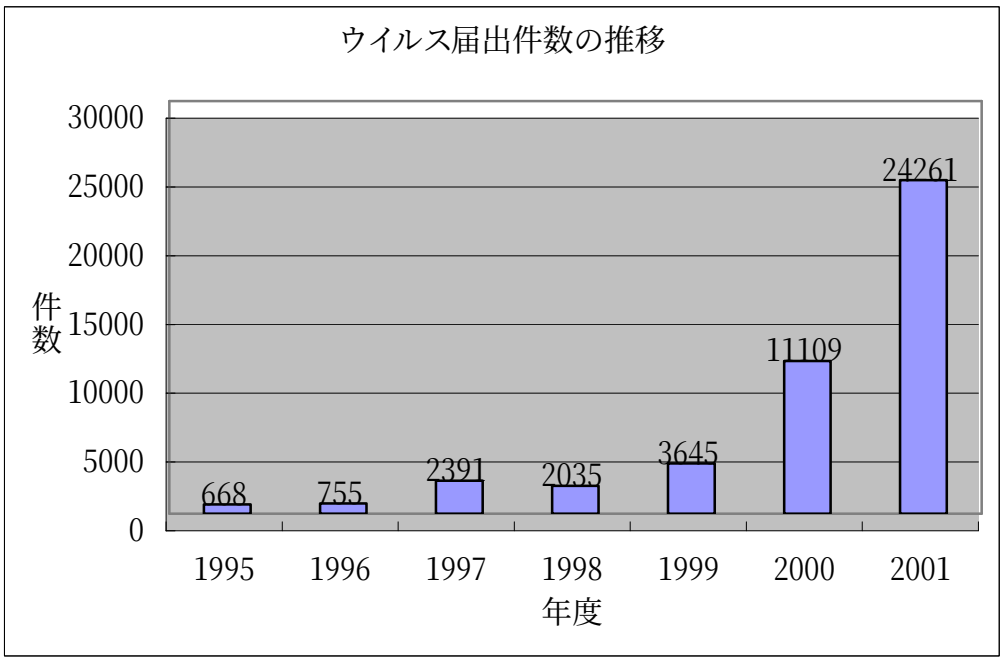
ワームとは別名を「インターネットワーム」といい、自らインターネットや電子メールを介して、他のパソコンに増殖・感染するプログラムのことである。他のプログラムに常駐することはなく、単独で活動する点とスクリプト言語などの簡易的な言語で作成される点などでウィルスとは異なる。

ウィルスとは他人のコンピュータに入り込んで、意図的に被害をもたらすプログラムと定義され、インターネットからダウンロードしたファイルや記憶媒体から感染する。

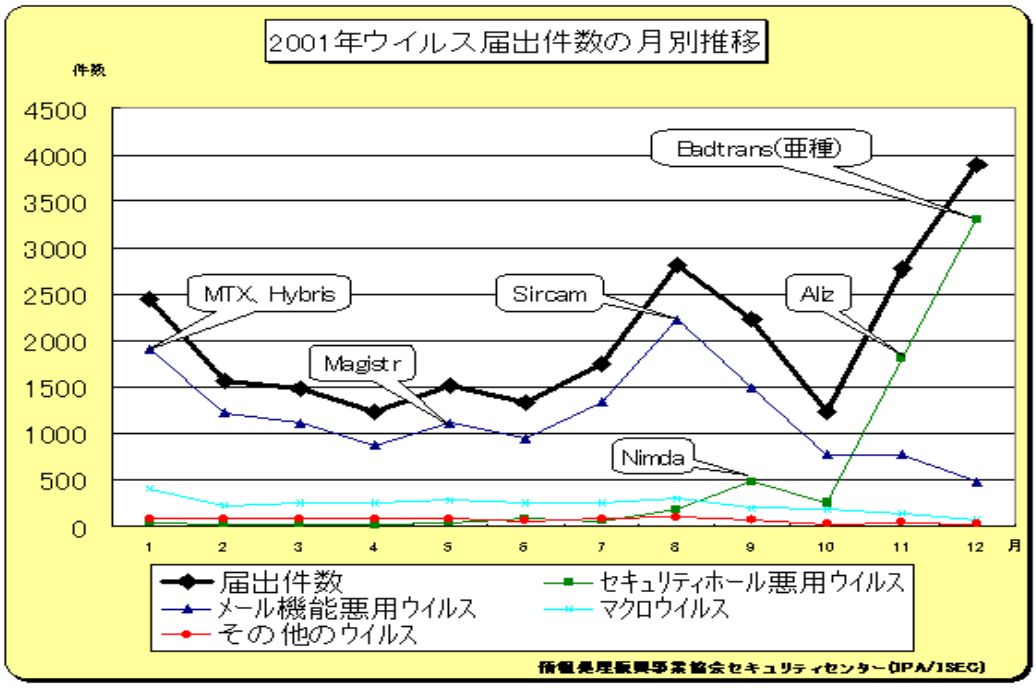
ここ数年世界的なインターネット・電子メールの普及に伴い、それらの数は爆発的に増えており、被害総額も甚大なものとなっている。（表＝米 Computer Economics 社調べ）



また、日本国内においても IPA（情報処理振興事業協会）の調査によれば、確実にウィルス・ワームの被害届出件数は増加しており、年々被害が増加していることを表している。（表）



このうち 2001 年度に特に届出の多かったものとして代表的なものとしては Nimda、Code Red、Sircam、BadTrans などがあげられる。 表=IPA 調べ）これらは主に電子メールやネットワークを介して感染し、ユーザのウィルスの認識も低かったせいかまたたくまに感染が広がった。特に Nimda はトレンドマイクロの調査によると、発生 2 週間で全世界の 170 万台以上のコンピュータに感染したと言われている。



表で紹介されたものを含めここ 1 年間の間で特に流行した代表的なワームとウィルスの解説を以下に示す。

(a) Nimda （ワーム）

2001 年 9 月 18 日に米トレンドマイクロ、McAfee AVERT などにより、警告が発せられた。危険度 「高」と設定され、爆発的な勢いで感染を広げた。原因としては、このワームがいかに上げられるような多くの感染経路を持つことが上げられる。

① 主に修正プログラムが適用されていないマイクロソフト社の IIS(Internet Information Server)サーバのセキュリティホールを突いて感染し、改ざんする。

② それを見たユーザのブラウザを通して、感染する。

③ ユーザが outlook 及び outlook express を使用していた場合、受信トレイを読み取り他のメールユーザに Nimda 自身のコピーを送信する。

④ 有効なネットワーク接続を探して、他のコンピュータにコピーを送信しようと試みる。また、NIMDA B、NIMDA C（ベンダーにより呼称は様々）など色々な亜種が登場しているのも特徴である。

(b) Code Red（ワーム）

2001 年 7 月 13 日以降に発見されたこのワームはマイクロソフト社の IIS(Internet Information Server)にあるセキュリティホールを利用し Web ページを改ざんする。さらに、ランダムに選択した IP アドレスのマシンにスキャンを行い、セキュリティホールのある IIS が稼動しているかどうか調べ、そのサーバに侵入しようと試みる。Nimda と同様にこちらも様々な亜種が登場している。

(c) Lion（ワーム）

2001 年 3 月 23 日に FBI（米連邦調査局）の NIPC（National Infrastructure Protection Center、社会基盤防衛センター）が警告。このワームは主に Linux 環境で活動し、そこで DNS サービスを提供する BIND アプリケーションのセキュリティホールを突いてくる。Lion は複数のファイルをバックドアに置き換え、さらにそれを利用するためマシンに侵入するためのパスワードファイルを攻撃元のハッカーに送信しようとする。

(d) Sircam（ウィルス）

このウィルスに対しては、2001 年 7 月 20 日以降の各セキュリティベンダーが警告を発した。メールで感染を広げるため、感染対象は Windows マシンであるが、使用しているメールソフトには依存していない。ウィルス・プログラムはメールに添付され、それを実行すると様々なファイルから収集したメールアドレスにウィルス自身を送信して感染を広げる。

(e) Bad Trans（ウィルス）

200 1年 11 月 26 日に McAfee AVERT より報告が出された。感染経路は電子メールのみである。このウィルスは Microsoft 社の Internet Explorer のセキュリティホールを突いて電子メールに添付されたプログラムを実行し、未開封の電子メールの差出人に勝手にウィルスつきメールを返信する。さらにトロイの木馬としても働き、ユーザ名やパスワードを作者のメールアドレスに送信する。

(f) Goner（ウィルス）

2001年12月5日に各セキュリティベンダーによって警告され、添付ファイルを実行すると多様な症状をだす。

① 電子メールやICQに添付されたファイルを実行すると、メールソフトのアドレス帳やICQ（インスタント・メッセージ・ソフト）に登録されている全てのユーザに自らを送信する。

② 特定のウィルス対策ソフトやパーソナル・ファイアーウォールのプログラムを削除する。

③ mIRCというインターネット・リレーチャット用ソフトの設定を変更しDos（Denial of Service）攻撃を仕掛ける。

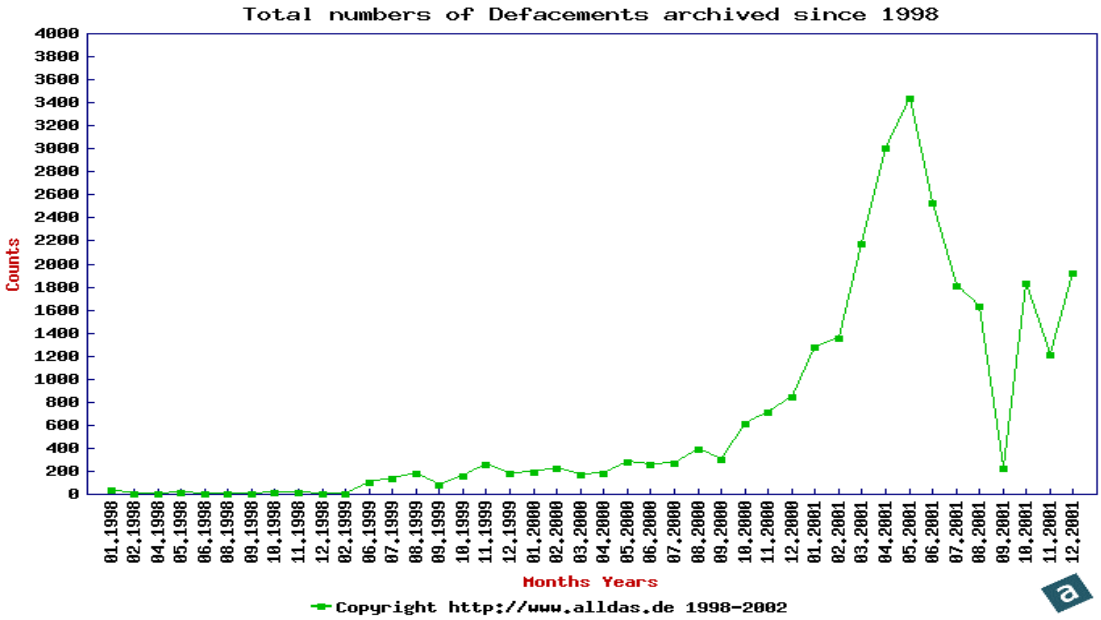
④ マシンが起動するたびウィルス・ファイルが実行されるようにレジストリを書き換える。主にOutlookを使用していなければメールを他のユーザに送信はしないが、それ以外のウィルス・プログラムの活動は行われてしまう。

(g) My party（ウィルス）

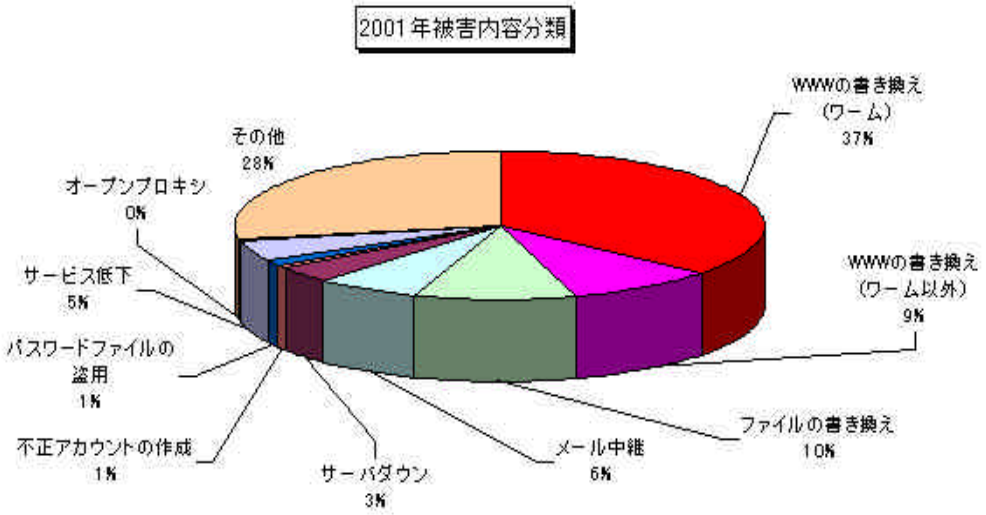
2002年1月28日から主に日本国内にて報告がよせられている。電子メールの添付ファイルで感染を広げる。この添付ファイルを実行すると、Windowsのアドレス帳に記載されたメールアドレスへウィルス添付メールを送信する。このウィルス・プログラム自身がメール送信機能を持つため、メールソフトに依存せずに感染を広げていく。

(2) Web改ざん

企業・自治体によるインターネット上の活動の増加に伴い、wwwサーバの改ざんが近年世界的に増加傾向にある（表＝alldas.de調べ）。その主な原因としては必要な修正モジュールをサーバに導入していない、サーバのセキュリティ設定ミスなどがあげられる。また、ワームに感染して改ざんされたとの報告も多い。

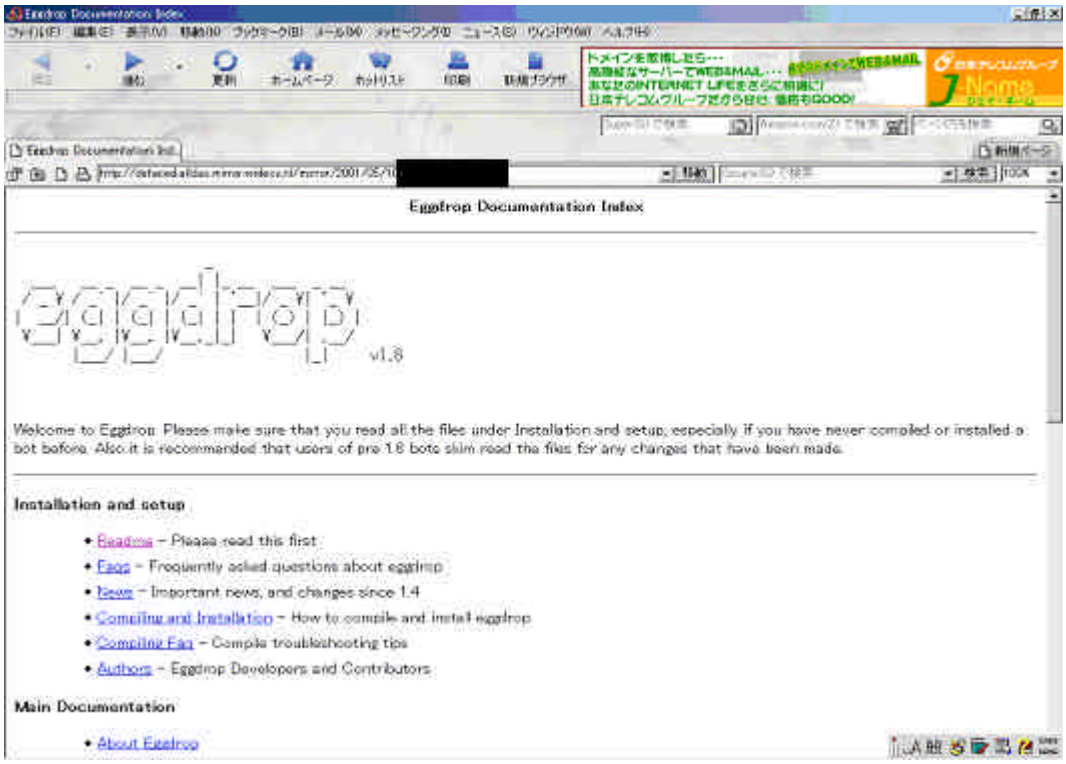


IPA に届けられた不正アクセス届出状況に被害内容の分類でも半数近くが www サーバの書き換えである。 表＝IPA 調べ）



改ざんされたサイトの例

(a) 某コンピュータメーカ（2001 年 5 月 10 日）



(b) 某服飾メーカ（2001 年 7 月 1 日）

(3) 個人情報流出

ワームとウィルスの被害状況、Web 改ざんと見てきたが、E コマースなどのインターネット上の企業活動が増えるにつれ、会員制サイトも増加している。それに伴って利用者の個人情報が流出するという問題が急増している。主な原因として、企業側の危機管理体制の甘さによるメールの誤送信による個人のメールアドレスの流出、サーバの設定ミスによる内部情報閲覧可能などの例あげられる。また cookie の偽造が出来てしまうクロスサイト・スクリプティングなどによる個人情報悪用・流出の危険性も度々報告されている。

(a) 事例① メール誤送信

2001 年 1 月 31 日に某テレビ局が、視聴者向けにメールを送信した際に、視聴者 1900 人分のメールアドレスを流出するという事件を発生させた。この事件に関して、同局ではお詫びの文章を Web サイト上に掲載している。原因としては、メールを BCC で送るべきところを CC で送信してしまい、メールアドレスが漏洩した。送信は、120 人から 250 人のメールアドレスを 9 回に分けて送ったがその際に、いずれも CC で送ってしまったとのことである。

(b) 事例② サーバの設定ミス

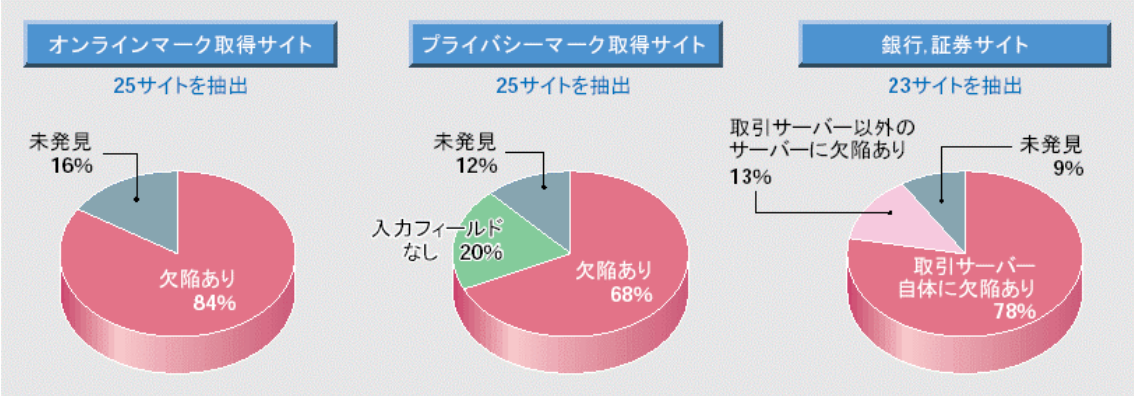
某学生向け就職情報サイトで、登録されている利用者の個人情報が、閲覧可能な状態であることが情報提供サービス会社の調べでわかった。この問題は同社によると、登録された情報が CSV (Comma Separated Values) ファイルで保存されており、保存先のディレクトリのパーミッション設定を適切に行っていなかったことによるものである。このディレクトリ内には、多数の CSV ファイルが保存されており、この CSV ファイルに氏名や連絡先を含む個人情報が 1 万人を超える規模で保存されていた。これらのファイルは、誰でも自由に閲覧が出来て、ダウンロードが可能な状態となっていた。

(c) 事例③ クロスサイト・スクリプティング

クロスサイト・スクリプティングとは、「www サイト側でのデータ・チェックが不十分なために、不正なスクリプトがターゲット www サイトに送りこまれた場合、その www サイトへアクセスしたユーザのブラウザにそのスクリプトを送信してしまう」という問題である。これを使えば、cookie 情報を盗んだり、それを利用してユーザになりすまして個人情報を盗み見できてしまう。

2001 年 10 月 18 日に発表された産業技術総合研究所のセキュリティ研究グループの

論文によると、きわめて多数の EC（電子商取引）サイトに、クレジットカードの情報入手や個人情報流出につながるセキュリティホールが存在するとの報告がなされた。社団法人 日本通信販売協会のオンラインマークを取得したサイトから 25 中 21 サイト（84%）と財団法人 日本情報処理開発協会のプライバシーマークを取得しているサイトからも 25 中 17 サイト（68%）がクロスサイト・スクリプティング対策を施していなかった。また、大手の銀行および証券サイトから23 サイト中 21 サイト（91%）はクロスサイト・スクリプティングが対策を実施していなかった。（表＝産業総合研究所調べ）



(4) 監視センターの記録から見る傾向

最近の攻撃の傾向を探るため、ハニーポットと呼ばれる故意に脆弱性を残したままにしたホストをインターネット上に設置しておき、それらのホストに対して実際に行われた攻撃を、snort（フリーで利用可能なネットワーク型侵入検知システム）を利用して記録した結果を集計する（記録は株式会社ラック提供）。集計する攻撃の記録は、2001 年 12 月 23 日から2002 年 2 月 16 日までのものであり、

① 攻撃手法

② 攻撃元（国と地域）

③ 日時

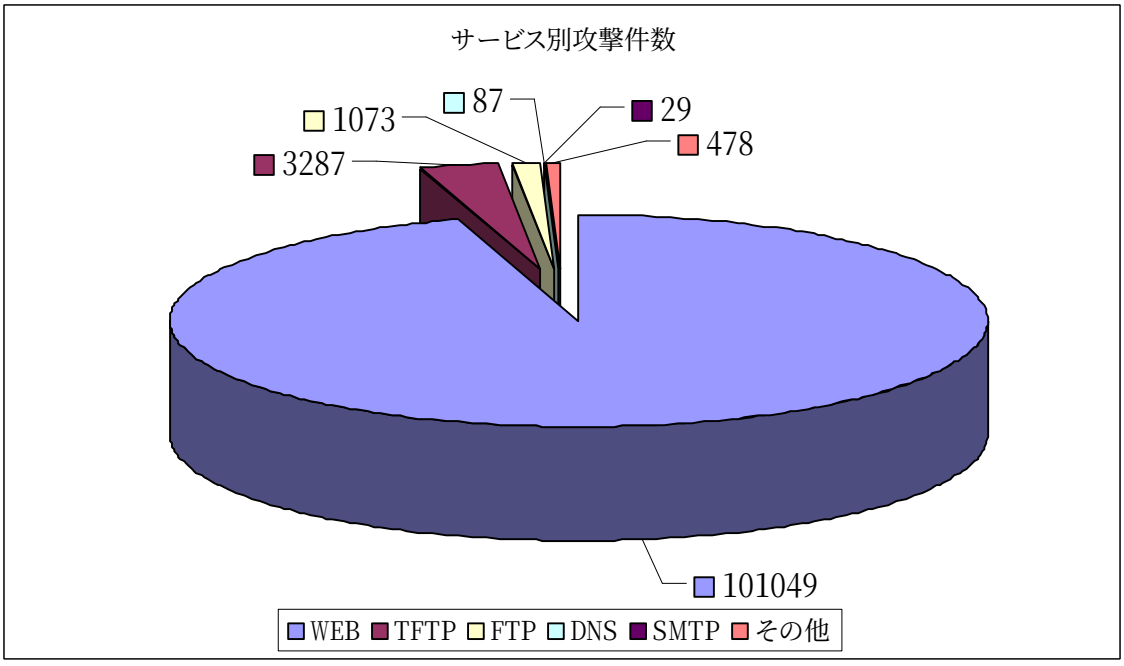
という3 つの観点から記録を集計し、最近の攻撃の傾向を探る。

(a) 攻撃手法から見た攻撃の傾向

侵入検知システムが検出した攻撃の記録を利用して、サービス別に攻撃件数の総数を集計すると下のグラフになる。また、攻撃手法別に件数を集計し、検出件数が多い順に整列させた表が「攻撃手法別件数（件数の多い順）」になる。

Web サービスへの攻撃が突出しているのは、Nimda ワームによる感染活動の影響である。TFTP の攻撃件数も同様に多いが、これは Nimda ワームに感染した結果、ワーム本体を TFTP プロトコルで転送する感染活動が記録された結果である。このことから、記録に見られる攻撃の大半は Nimda ワームによるものであることがわかる。

また、Nimda ワームの攻撃による記録に次いで FTP サービスへの攻撃が多いが、これは Wu-Ftpd に見つかっているセキュリティホールを利用して侵入しようとした攻撃が記録された結果である。昨年、一昨年とリモートから侵入可能な問題が見つかっており、また攻撃用ツールが公開されているため、ツールを入手した多くの攻撃者が侵入に利用したものと思われる。DNS サービスへの攻撃は、DNS サービスのバージョン情報を調べる手法であるが、調査したのみで攻撃が行われた記録はない。また、SMTP サービスはアカウント情報を収集する攻撃手法が記録されていた。



それぞれの攻撃手法を件数が多い順に並べると以下の表になる。Nimda ワームによる攻撃で記録されるイベントは、

- WEB IIS cmd.exe access
- WEB IIS multiple decode attempt
- WEB IIS scripts access

- WEB-IIS CodeRed v2 root.exe access
- WEB-FRONTPAGE /_vti_bin/ access
- WEB-IIS _mem_bin access
- TFTP GET Admin.dll

であり、非常に多く記録されているのが以下の表から覗える。

また、20件前後でWeb関連の多数の攻撃手法が記録されているが、このことからWebサーバ、CGI等のセキュリティホールを確認するツールによる攻撃が20回程度あったことが推測される。それらのツールは網羅的に既知のセキュリティホールを確認するため、多くの種類の攻撃が記録に残り攻撃があったことが推測しやすい。

表 攻撃手法別件数（件数の多い順）

件数	攻撃手法	サービス
64047	WEB IIS cmd.exe access	WEB
9886	WEB IIS multiple decode attempt	WEB
9290	WEB IIS scripts access	WEB
6254	WEB MISC 403 Forbidden	WEB
5095	WEB FRONTPAGE /_vti_bin/ access	WEB
5013	WEB IIS CodeRed v2 root.exe access	WEB
3271	TFTP GET Admin.dll	TFTP
428	FTP EXPLOIT wu ftpd 2.6.0 site exec overflow	FTP
405	ATTACK RESPONSES http dir listing	ATTACK
353	FTP site exec	FTP
225	FTP EXPLOIT wu ftpd 2.6.0 site exec format string check	FTP
170	WEB IIS Overflow htr access	WEB
105	WEB MISC order.log access	WEB
105	WEB MISC http directory traversal	WEB
60	MISC Large ICMP Packet	MISC
51	WEB CGI php access	WEB
51	WEB CGI aglimpse access	WEB
45	DNS named version attempt	DNS
42	DNS named iquery attempt	DNS
33	WEB IIS File permission canonicalization	WEB
29	WEB CGI wrap access	WEB
29	WEB CGI campas access	WEB
29	FTP EXPLOIT format string	FTP

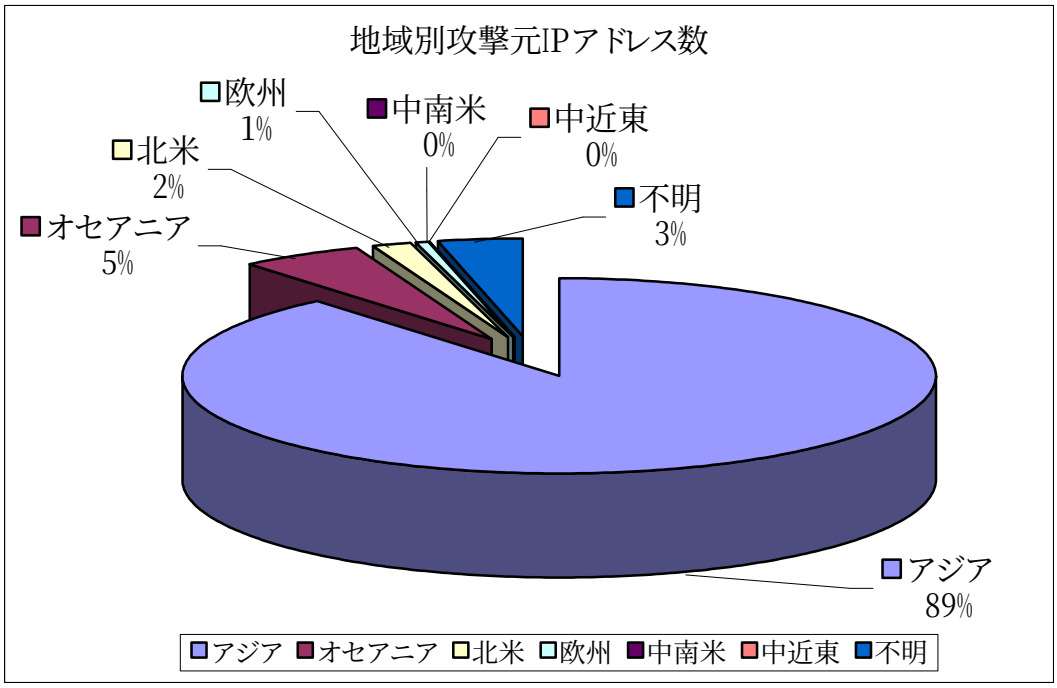
28	WEB CGI win c sample.exe access	WEB
28	WEB CGI nph test cgi access	WEB
27	WEB CGI uploader.exe access	WEB
26	WEB IIS .bat? access	WEB
26	WEB CGI websendmail access	WEB
26	WEB CGI phf access	WEB
25	WEB MISC handler access	WEB
25	WEB CGI view source access	WEB
25	WEB CGI test cgi access	WEB
23	WEB IIS asp dot attempt	WEB
23	WEB IIS ISAPI .idq access	WEB
23	WEB CGI wwwboard passwd access	WEB
22	WEB MISC webdist.cgi access	WEB
22	WEB MISC cachemgr.cgi access	WEB
22	WEB MISC /etc/passwd	WEB
22	WEB IIS newdsn.exe access	WEB
22	WEB IIS msadc/msadcs.dll access	WEB
22	WEB FRONTPAGE users.pwd access	WEB
22	WEB CGI whoisraw attempt	WEB
22	WEB CGI survey.cgi access	WEB
22	WEB CGI faxsurvey access	WEB
21	WEB MISC /cgi bin/jj attempt	WEB
21	WEB IIS site server config access	WEB
21	WEB IIS showcode.asp access	WEB
21	WEB IIS showcode access	WEB
21	WEB IIS codebrowser Exair access	WEB
21	WEB FRONTPAGE service.pwd	WEB
21	WEB FRONTPAGE authors.pwd access	WEB
21	WEB FRONTPAGE administrators.pwd	WEB
21	WEB FRONTPAGE _vti_rpc access	WEB
21	WEB CGI wwwadmin.pl access	WEB
21	WEB CGI visadmin.exe access	WEB
21	WEB CGI bnbform.cgi access	WEB
21	WEB CGI NPH publish access	WEB
21	SMTP expn decode	SMTP
20	WEB MISC PageService access	WEB
19	FTP EXPLOIT wu ftpd 2.6.0 linux overflow	FTP
17	WEB CGI formmail access	WEB
17	WEB CGI filemail access	WEB
16	TFTP root directory	TFTP
14	WEB IIS ISAPI .ida attempt	WEB
13	WEB CGI maillist.pl access	WEB
13	ATTACK RESPONSES id check returned root	ATTACK
11	FTP EXPLOIT wu ftpd 2.6.0 site exec format string overflow Linux	FTP

9	WEB IIS _mem_bin access	WEB
8	WEB FRONTPAGE fourdots request	WEB
8	SMTP RCPT TO overflow	SMTP
5	WEB MISC sadmind worm access	WEB
5	WEB IIS ISAPI .ida access	WEB
4	WEB MISC whisker splice attack	WEB
4	FTP wu ftp file completion attempt {	FTP
4	FTP wu ftp file completion attempt [	FTP
1	WEB IIS .... access	WEB
1	WEB FRONTPAGE shtml.exe	WEB
1	WEB FRONTPAGE shtml.dll	WEB

(b) 攻撃元の国から見た攻撃の傾向

攻撃者が利用しているIP アドレスから、そのIP アドレスが割り当てられている国を調査し、それぞれの国が属する地域ごとに攻撃元 IP アドレス数を集計してみる。この結果から、世界のどの地域から攻撃が行われているかが判断できる。

集計結果を見るとアジア地域からの攻撃が圧倒的に多いが、これは Nimda ワームが、感染している自身のホストのIP アドレスに近いIP アドレスを次の感染先に選ぶためであり、攻撃を記録している侵入検知システムおよびハニーポットが設置されているネットワークが、アジアで利用されているIP アドレスに近かったからであると思われる。また、攻撃者は自分の攻撃元を隠すために、他のコンピュータを踏み台にしている可能性もあるので、攻撃元 IP アドレス＝攻撃者のコンピュータ図式が必ずしも成立しない点にも注意が必要である。



以下に各国別の攻撃元 IP 数を挙げる。アジアではタイが 1番多く798となっている。また、バングラデシュ、スリランカといったインターネットの普及があまり進んでいないと思われる国からも数件の攻撃が記録されている。また、IT 産業が発展しているヨーロッパ、および北米からの攻撃が少ないことは意外である。

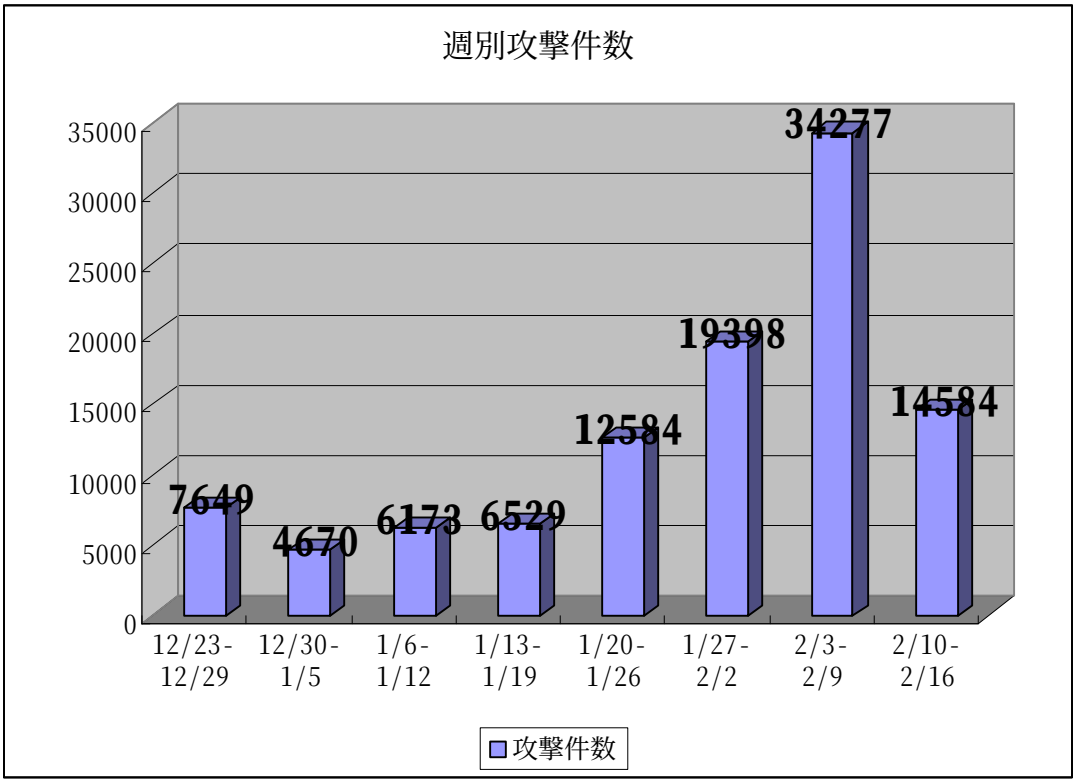
表 国別の攻撃元 IP 数

攻撃元 IP 数	コード	国名	地域
54	Unknown	-	-
798	TH	タイ	アジア
233	KR	韓国	アジア
89	TW	台湾	アジア
63	IN	インド	アジア
52	JP	日本	アジア
40	CN	中華人民共和国	アジア
31	SG	シンガポール	アジア
16	HK	香港	アジア
16	PK	パキスタン	アジア
14	MY	マレーシア	アジア
9	ID	インドネシア	アジア
8	LK	スリランカ	アジア
5	BD	バングラデシュ	アジア
2	KH	カンボジア	アジア

1	PH	フィリピン	アジア
78	AU	オーストラリア	オセアニア
4	NZ	ニュージーランド	オセアニア
2	IT	イタリア	欧州
2	SE	スウェーデン	欧州
1	DE	ドイツ	欧州
1	ES	スペイン	欧州
1	GB	イギリス	欧州
1	NL	オランダ	欧州
1	IL	イスラエル	中近東
1	AR	アルゼンチン	中南米
1	BR	ブラジル	中南米
1	PE	ペルー	中南米
20	US	アメリカ合衆国	北米
4	CA	カナダ	北米

(c) 週別での攻撃の傾向

週ごとでの攻撃件数を週計した結果が下のグラフである。年を越す週が最も件数が少ないことがわかる。2月 3日から2月 9日までの件数が突出しているが、この件数は後のワームの攻撃件数を週別で示したグラフから分かるが Nimda ワームによるものであり、新しいセキュリティホールが見つかりその問題を利用した攻撃が増加したなどの特別の意味を持つものではない。



上記のグラフだけではどのサービスへの攻撃手法が多く利用されているかが不明なため、攻撃手法を以下のカテゴリにわけ、それぞれの件数をグラフ化する。分類するカテゴリは、

① Nimda ワーム（以下の攻撃手法を含む）

- WEB-IIS multiple decode attempt
- WEB-IIS scripts access
- WEB-IIS cmd.exe access
- WEB-IIS CodeRed v2 root.exe access
- TFTP GET Admin.dll
- WEB-IIS CodeRed v2 root.exe access
- WEB-FRONTPAGE /_vti_bin/ access

② Code Red ワーム（以下の攻撃手法を含む）

- WEB-IIS ISAPI .ida attempt
- WEB-IIS ISAPI .ida access
- WEB-IIS ISAPI .idq access

③ FTP サービスへの攻撃（FTP 全般）

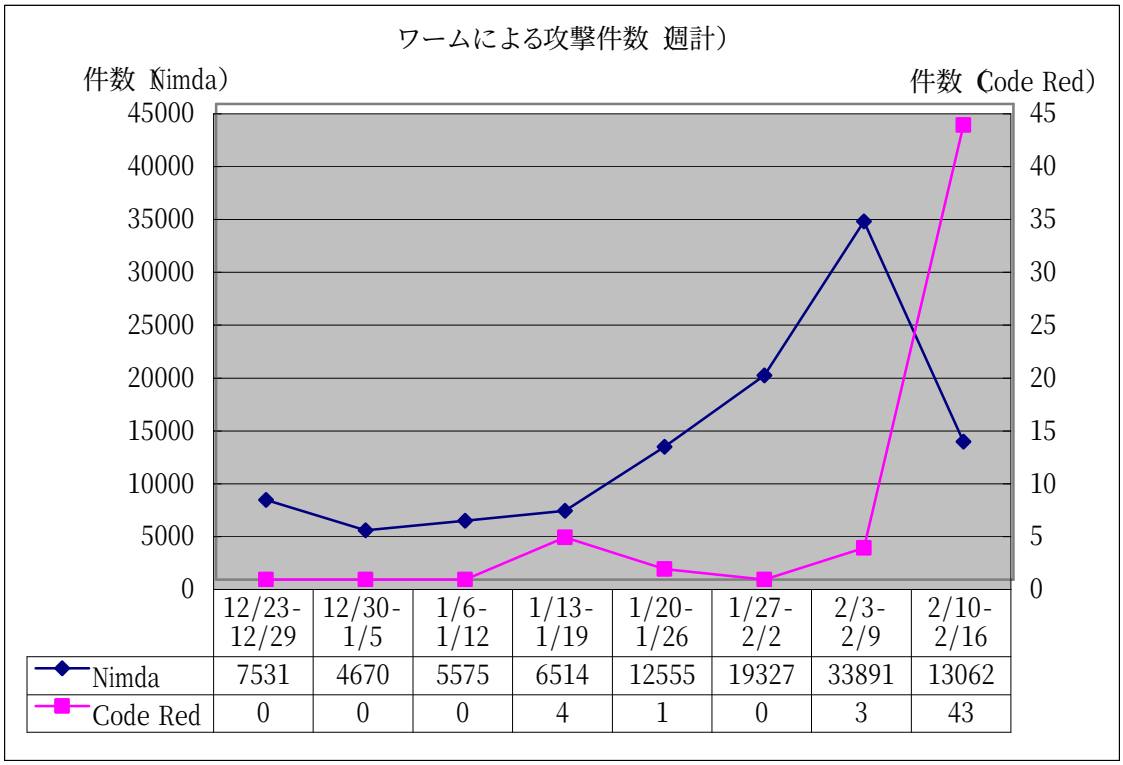
④ SMTP サービスへの攻撃（SMTP 全般）

⑤ DNS サービスへの攻撃（DNS 全般）

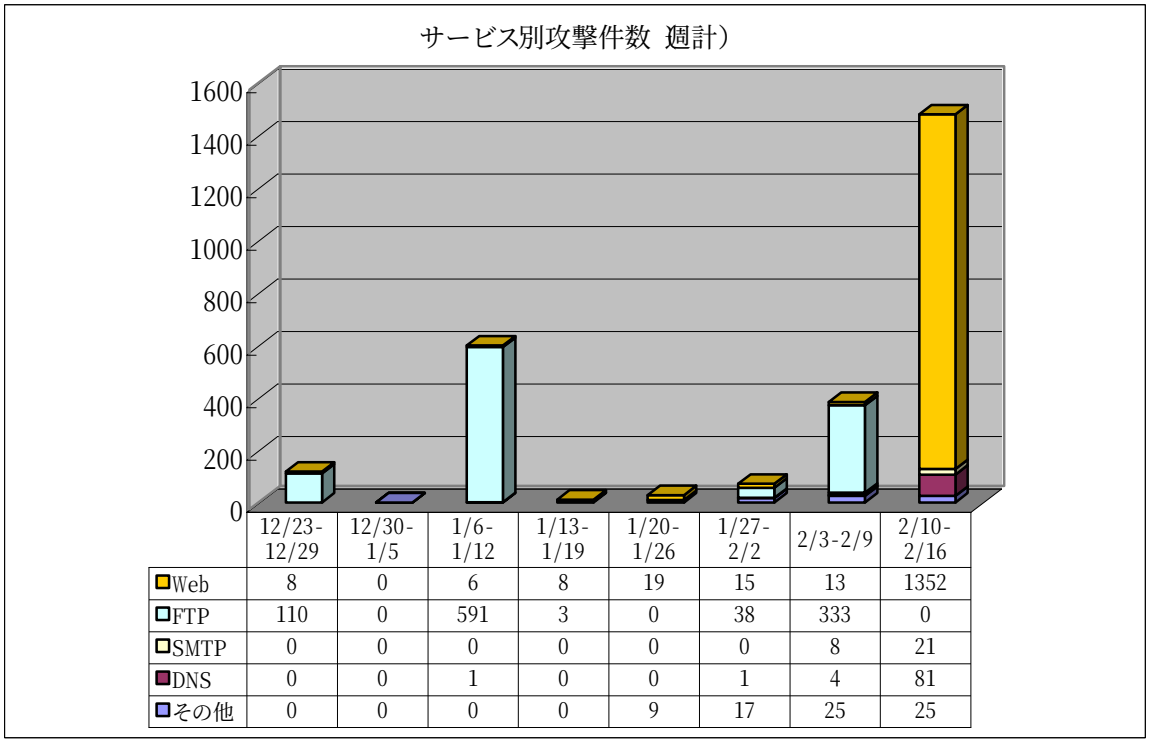
⑥ Web サービスへの攻撃（Web 全般）

⑦ その他

の 7つとする。ただし、ワームによる攻撃は自動で行われている感染活動であり、攻撃者による攻撃と分けて分析した方が攻撃の実体を見極めやすい。そこで、Nimda ワームとCode Red ワームは別個にワームによる攻撃件数として集計し、サービス別の攻撃手法とは分けて集計する。



	12/23-12/29	12/30-1/5	1/6-1/12	1/13-1/19	1/20-1/26	1/27-2/2	2/3-2/9	2/10-2/16
Nimda	7531	4670	5575	6514	12555	19327	33891	13062
Code Red	0	0	0	4	1	0	3	43



	12/23-12/29	12/30-1/5	1/6-1/12	1/13-1/19	1/20-1/26	1/27-2/2	2/3-2/9	2/10-2/16
Web	8	0	6	8	19	15	13	1352
FTP	110	0	591	3	0	38	333	0
SMTP	0	0	0	0	0	0	8	21
DNS	0	0	1	0	0	1	4	81
その他	0	0	0	0	9	17	25	25

ワームによる攻撃の記録と攻撃者による攻撃の記録を分けたことで、週別攻撃件数のグラフで見られた傾向を作っていたのはワームによる感染活動の増減の結果であったことがわかる。ワームによる攻撃を除く、攻撃者が手動またはツールを利用して行われた攻撃の傾向は、「サービス別攻撃件数（週計）」に見られるとおりである。このグラフを見ると、FTP への攻撃が定期的に行われているのがわかる。また、2002 年 2 月 10 日～2002 年 2 月 16 日の週には、Web サーバに対して多数の攻撃が行われたことが分かる。

2. 不正アクセス行為の手口

(1) バッファ・オーバーフロー

(a) 概要

バッファ・オーバーフローを利用した攻撃は、1980 年代の中ごろからその問題が指摘されており、1990 年代になって実際にバッファ・オーバーフローの問題を利用してプログラムの制御を奪う攻撃ツールが多数公開され、またその詳細を記述した技術文書も発表され、その危険性が広く認識されるようになった。それ以降、著名なサーバ・アプリケーションから無名のアプリ

ケーションまで、非常に多くのアプリケーションにバッファ・オーバーフローの問題は発見され、クラッカーによる不正アクセス行為等に利用されている。

バッファ・オーバーフローの問題を利用した攻撃の脅威は、動作しているプログラムの制御を奪い、攻撃者が送り込んだ機械語コードが代わりに実行されてしまう点にある。

バッファ・オーバーフローの問題は日々発見／報告されており、2001 年に見つかったバッファ・オーバーフローの問題の総数は 78 件にのぼり、2002 年に入ってからも 2 月末までで 11 件の問題が報告されている 株式会社ラック SNSDB 調べ)。バッファ・オーバーフローの問題を利用した攻撃の手口を以下の 3つに分類し、2001 年 1 月～2002 年 2 月までの報告件数を月ごとに集計しグラフ化する。

① リモートからの攻撃に利用

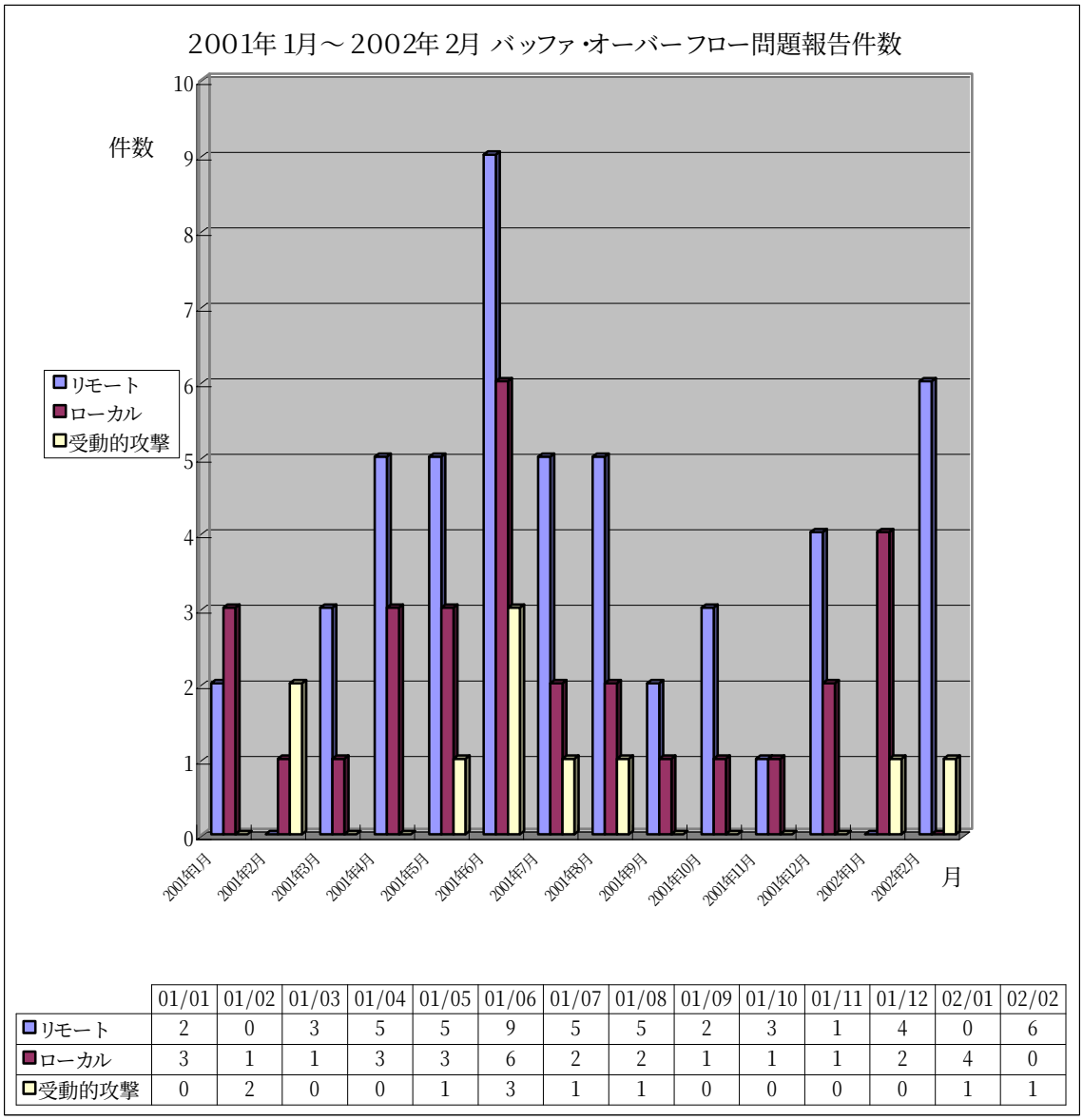
攻撃者がネットワーク越しに侵入する際に利用する。攻撃者が攻撃対象のマシンからネットワークを介して離れた場所にいるために「リモートからの攻撃」と呼ばれる。サーバ・アプリケーションなどに問題が見つかった問題がこれに該当し、攻撃者はネットワーク越しにサーバ・アプリケーションに接続し、攻撃を行い侵入する。

② ローカルでの攻撃に利用

攻撃者が攻撃対象のシステムにログインしている状態で、一般ユーザから特権ユーザに権限を上昇させる際に利用する。攻撃対象となるマシン上で攻撃を行うため「ローカルでの攻撃」と呼ばれる。

③ 受動的な攻撃に利用

通常の攻撃は攻撃者が能動的に行うが、攻撃対象の行動を元に開始する攻撃を受動的攻撃という。たとえば、悪意のある Web サイトにアクセスする、メールを受信する、ファイルを開くといったユーザの行動によって、バッファ・オーバーフローの問題が発生し攻撃が開始される。



	01/01	01/02	01/03	01/04	01/05	01/06	01/07	01/08	01/09	01/10	01/11	01/12	02/01	02/02
リモート	2	0	3	5	5	9	5	5	2	3	1	4	0	6
ローカル	3	1	1	3	3	6	2	2	1	1	1	2	4	0
受動的攻撃	0	2	0	0	1	3	1	1	0	0	0	0	1	1

さらに、ここ最近発見されたバッファ・オーバーフローの問題でをいくつか紹介する（株式会社ラック SNSDB 調べ）。

①Microsoft Internet Explorer HTML Document Directive Buffer Overflow Vulnerability

・発見日　　2002 年 2 月 7 日

・発見者　　dH team and SECURITY.NNOV

・影響のある製品

Internet Explorer 5.5

Internet Explorer 5.5 SP1

Internet Explorer 5.5 SP2

Internet Explorer 6.0

・問題

Microsoft Internet Explorer が利用している mshtml.dll に、バッファ・オーバーフローの問題が存在する。攻撃者は巧妙に Web ページを作成することで、ユーザのシステム上で任意のコードが実行できる可能性がある。ユーザは悪意のあるサイトを訪問し、コンテンツを参照することで、システム上で悪意のあるコードが実行される可能性がある。

② Solaris libsldap Buffer Overflow Vulnerability

・発見日　2001 年 6 月 26 日

・発見者　Jouko Pynnonen

・影響のある製品

Solaris 8 SPARC

Solaris 8 i386

・問題

Solaris には、LDAP(Lightweight Directory Access Protocol)を実装するライブラリが同胞されている。環境変数 LDAP_OPTIONS に長い値が設定されることで、バッファ・オーバーフローの問題が発生する。

③ MS Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability

・発見日　2001 年 6 月 18 日

・発見者　eEye Digital Security

・影響のある製品

Windows NT 4.0 SP6a + Internet Information Server 4.0

Windows 2000 + Internet Information Service 5.0

Windows 2000 SP1 + Internet Information Service 5.0

Windows 2000 SP2 + Internet Information Service 5.0

・問題

IIS から ISAPI エクステンション機能を利用して呼び出される idq.dll にバッファ・オーバーフローの問題がある。「idq」および「ida」という拡張子のスクリプトを IIS から参照する際に、パラメータに長い文字列を設定することで、バッファ・オーバーフローの問題が発生する。これは、CodeRed ワームで利用された脆弱性である。

(b) 仕組み

バッファ・オーバーフローの問題は、C 言語で作成されたプログラム上で、文字列の長さをチェックすることなく変数間でコピーする際に生じる。「コピー元の変数の文字数がコピー先の変数の文字数を超えているか否か」という文字列の長さのチェックを怠ることで、プログラムが確保している変数の領域を超えて文字列をコピーし、本来関係のないメモリ内容を上書きする現象を一般にバッファ・オーバーフローと呼ぶ。確保した領域（バッファ）を、溢れ（オーバーフロー）させるので、このような名称になっている。また、この現象がメモリ上のスタックと呼ばれる領域で発生することから、他の領域のオーバーフロー問題と区別して「スタック・バッファ・オーバーフロー」と呼ばれることもある。

バッファ・オーバーフローによりメモリの内容が上書き、つまり破壊されてしまうと、プログラムはデータの整合性に齟齬をきたし異常終了することになる。特に、ユーザから受け取った文字列を処理する部分にバッファ・オーバーフローの問題がある場合、プログラムに渡す文字列を巧妙に組み立てることでスタック領域に格納されているリターンアドレスを上書きし、そのプログラムの制御を奪うことができる。プログラムの制御を奪うとは、自分が処理させたいことをそのプログラムに実行させることができることを意味し、「任意のコードが実行できる」と表現される場合もある。

バッファ・オーバーフローの問題を利用した攻撃の影響は、問題の見つかったアプリケーションによって異なる。

① サーバ・アプリケーションの場合

Web サーバ、SMTP サーバなどのサーバ・アプリケーションに、バッファ・オーバーフローの問題が存在する場合、攻撃者はネットワーク越しにサービスにアクセスし、バッファ・オーバーフローの問題を利用してプログラムの制御を奪い、シェルプログラムを実行したり、バックドアを作成したりすることで、ログイン等を経ることなく侵入することが可能となる。ネットワーク越しに簡単に侵入できるため、影響は非常に大きい。

ただし、必ずしも管理者権限で侵入することができるとは限らない。どの権限で侵入できるかは、制御を奪ったサーバ・アプリケーションの権限によるからである。そのため、最近のサーバ・アプリケーションでは、管理者権限が必要な処理に限って管理者権限で動作させ、通常は一般ユーザ権限で動作するような仕様となっており、万が一バッファ・オーバーフローの問題が発見され、侵入に利用されたとしても管理者権限が渡らないようにしているものが多い。

② ローカル・アプリケーションの場合

ユーザがログイン後にローカルシステム上で実行するプログラムに存在するバッファ・オーバーフローの問題の場合、サーバ・アプリケーションの場合のようにプログラムの制御を奪って任意のコードを実行させることだけが目的ではなく、主たる目的は権限の上昇にある。なぜなら、ローカル・アプリケーションの場合は既にログインしているため、攻撃者は単純にコマンド実行であればシェルから実行することができるからである。

権限を上昇させるためには、そのアプリケーションにバッファ・オーバーフローの問題が存在するだけでなく、SetUID のパーミッションが設定されている必要がある。SetUID のパーミッションが設定されているプログラムを実行すると、そのプログラムが動作している間は一時的にそのファイルの所有者と同じ権限になる。これは、root しか参照／編集することのできないファイルなどを一般ユーザが一時的に利用する場合に、設定されている（例：passwd コマンドなど）。そのため、root が所有者で SetUID のパーミッションが設定されているアプリケーションにバッファ・オーバーフローの問題が存在した場合、プログラムの実行中は root 権限になるため、プログラムの制御を奪うことで権限を root に上昇させることができるようになる。

(c) 対策

バッファ・オーバーフローの対策としては、プログラムの作成時にバッファ・オーバーフローの問題を持つようなプログラムを作成しないという方法がある。バッファ・オーバーフローを引き起こす、つまり文字数をチェックせずに文字列の処理を行うC 言語の標準関数は特定されている、それらを利用せず他の文字数チェックの仕組みも持つ関数を利用するのである。これを実現するためには、①プログラマの教育、②プログラムのテスト、③ソースコードチェックなどの体制が必要になる。

一方、バッファ・オーバーフローの発生を前提としてそれを防ぐための機構も開発されている。

・StackGuard （http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/）

・libsafe （http://www.avayalabs.com/project/libsafe/index.html）

・Sun Solaris Stack Protection

などが代表的なものである。それぞれ異なる視点から対策方法をとっており、StackGuard は、バッファ・オーバーフローによって他のメモリ領域が上書きされた現象を検出する仕組みを採用している。libsafe は、バッファ・オーバーフローの問題を生じさせるC 言語の標準関数をより安全な関数に置き換えるという視点から対策を行っている。Sun 社が提供しているSolaris というオペレーティング・システム（SPARC 上で動作するバージョン）には、メモリのスタック領域から実行権限を削除することができる機能がある。これにより、バッファ・オーバーフローの問題を利用した攻撃の多くは、スタック上に自分の実行したいコードを保存しておき、プログラムの制御を奪った後そのコードを実行させるため、スタック領域から実行権限を削除しておけば、バッファ・オーバーフローの発生およびプログラムの制御の奪取は防ぐことができないが、その後のコードの実行を防ぐことができる。ただし、これらの仕組みには回避策もあり、機構としてバッファ・オーバーフローを防ぐ完全な対策というものはないのが現状である。

(2) 受動的攻撃

(a) 概要

受動的攻撃とは、「攻撃者が攻撃の主導権を持っているものの、攻撃の発生が被攻撃者の行動による攻撃手法」のことである。たとえば、攻撃者は攻撃を行うための Web サイトを用意しておき、そこにアクセスしてきたクライアントが悪意のあるコンテンツを参照すると攻撃が発生しクライアントが被害にあうというような攻撃である。攻撃者は、準備はするけれども積極的には攻撃を仕掛けない点が、従来の攻撃方法と異なる。また、その特性上、攻撃者の狙いはクライアントである。これも、通常の「能動的」攻撃は侵入を目的としており、攻撃者の狙いがサーバである点と異なる。

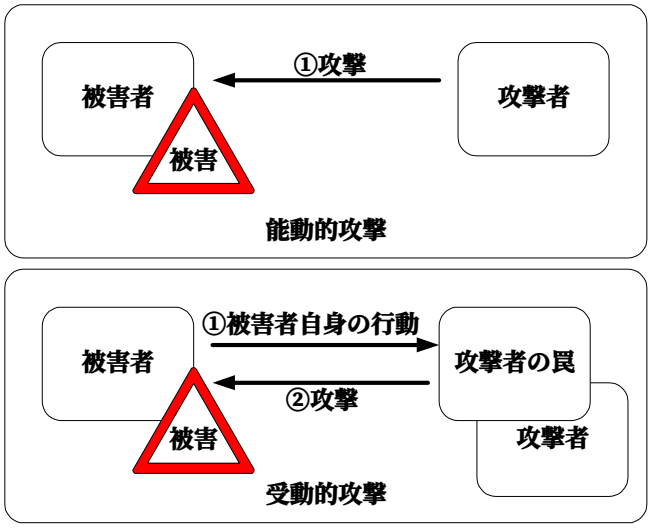
この手の攻撃手法は近年増加しており、シマンテック社による 2001 年 9 月の「Symantec Security Response」の報告によれば、Microsoft VM のセキュリティホールを利用したてWeb サイトにアクセスしたクライアントに対してウィルスを感染させたり、大量のメールを勝手に送信したりする受動的攻撃（シマンテック社はこの攻撃手法を「JS.Exception.Exploit」という名前

でウィルスリストに追加している)が Nimda を抜いて 1 位になったと報告しており、多くのインターネット利用者が知らないうちに攻撃の被害にあっている可能性があるものと思われる。

(b) 仕組み

受動的攻撃の対極にある攻撃手法を能動的攻撃とよぶことがあるが、2つを対比すると能動的攻撃は「攻撃者によって直接的に攻撃が行われる」のに対して、受動的攻撃は「攻撃者によって間接的に攻撃が行われる」と表現することができる。この 2種類の攻撃手法は多くの場合能動的攻撃を単に攻撃と呼び、もう一方を受動的攻撃と呼ぶことが多いようである。この 2種類の攻撃を、攻撃者と被害者それぞれの行動を中心に捉えた場合、図1のような違いがあることがわかる。

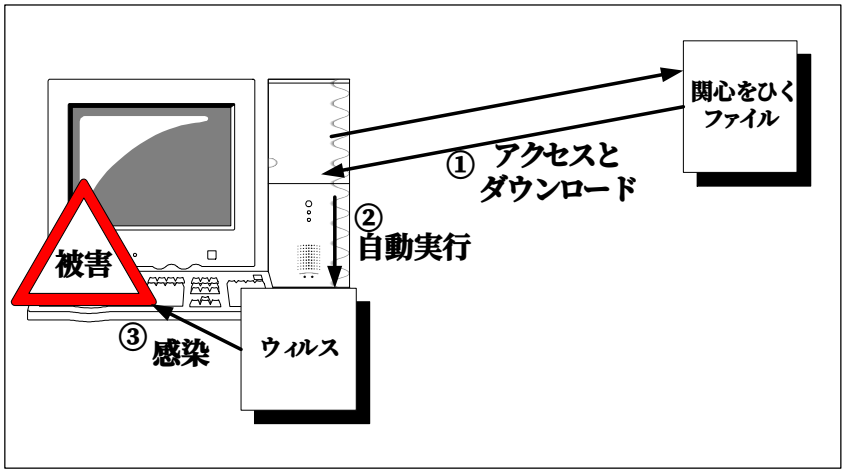
図 能動的攻撃と受動的攻撃



能動的攻撃では、攻撃行為が攻撃者によって直接行われるのに対して、受動的攻撃では、それが被害者の行動をきっかけとして行われている。

① 受動的攻撃の例 1

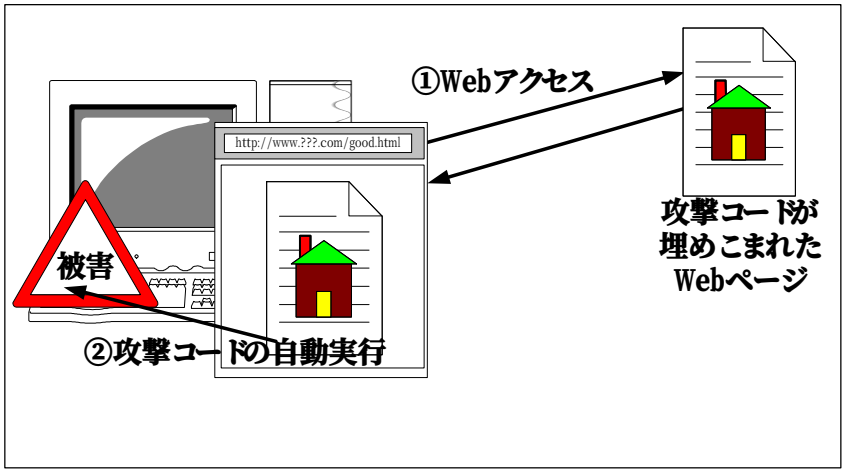
以下の図はファイルダウンロードによって受動的攻撃が行われている例である。



攻撃者がウィルスに感染したファイルを、通常のファイルを偽装して公開している。そして、そのファイルを被害者が興味を抱いてダウンロードする。すると、ダウンロード後、ファイルが自動実行されてウィルスに感染してしまう。

② 受動的攻撃の例２

以下の図は Web アクセスを利用して受動的攻撃が行われている例である。



攻撃者が悪意のあるサイトを公開している。その中のコンテンツを参照すると、コンテンツに組み込まれている攻撃コードが実行されて、攻撃が行われる。

これらの 2つの例に共通している点が 2つある。1つは、受動的攻撃の特徴としてすでに説明している通り、 攻撃行為が被害者の行動をきっかけとして行われている点」である。そし

てもう一つは、「攻撃者が直接攻撃を行っていないにも関わらず、攻撃の主導権を攻撃者が持っている点」である。「受動的攻撃の例 1」で、もしファイルの実行が自動で行われず、「ファイルを開く、実行する」という被害者の行動が必要であるならば、「受動的攻撃の例 1」は受動的な手法を用いているが、受動的攻撃と呼ぶことはできない。なぜなら、攻撃が成立するために必要な最後の行動を被害者にゆだねているからである。

受動的攻撃には、攻撃のきっかけが被害者によっておこなわれるため、クライアント・アプリケーションのバグを利用する場合が多い。たとえば Microsoft Internet Explorer の「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する(MS01-020)」問題や、Apple 社の Quick Time Player の「Content-Type Remote Buffer Overflow Vulnerability」問題などは、代表的なクライアント・アプリケーションのバグである。また、Web サイトへのアクセスを利用した「クロスサイト・スクリプティング」という問題の報告が相次いでいる。

「受動的攻撃の脅威」は、被害者の行動がきっかけとなりながら攻撃の主導権を攻撃者が持っているという受動的攻撃の特徴が、まさしくその脅威であると考えられる。被害者の行動、たとえば Web アクセスや電子メールのプレビュー、ファイルのダウンロードなどがきっかけとなるため、不正アクセス対策として一般化しつつあるファイアウォールによるネットワークの保護などが無効化されてしまう危険性がある。そのため、不正アクセス対策が施されたネットワークへの侵入方法として「受動的攻撃」は将来において、増加する危険性を秘めているといえる。

(c) 対策

受動的攻撃を防ぐためには、攻撃に利用されるクライアント・アプリケーションのセキュリティホールを解決する必要がある。個人の場合には、自分の管理するマシンにセキュリティホールを解決するためのパッチを適用すればよいが、大規模な組織ではシステム管理者は全てのユーザに、パッチの適用、バージョンアップを行わせる必要があり、大規模になればなるほどその徹底は難しい。そのため、セキュリティポリシーとポリシーを実現するための体制が必要になると考えられる。

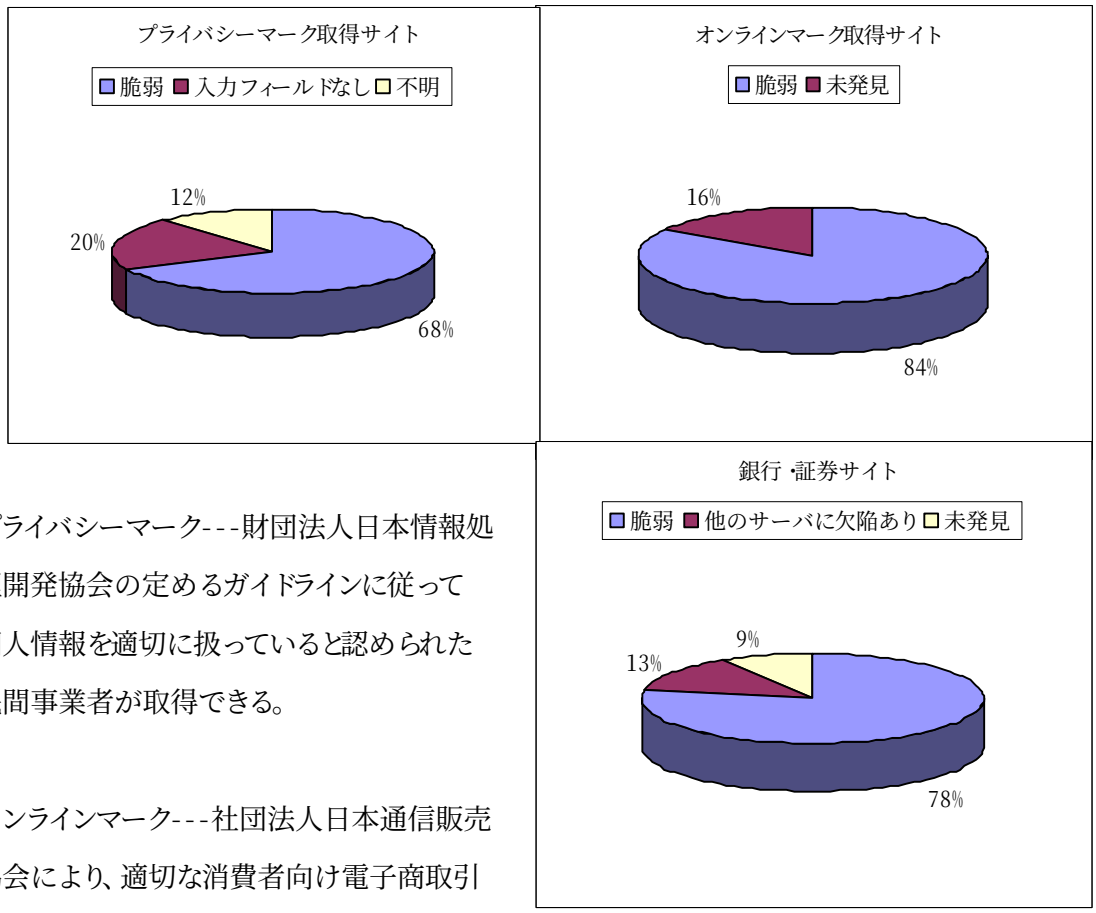
(3) クロスサイト・スクリプティング

(a) 概要

クロスサイト・スクリプティングとは、EC（E-Commerce）サイトを中心に、個人情報漏洩やなりすましを引き起こす web アプリケーションが抱える脆弱性のことである。

この脆弱性は2000年2月にアメリカのインターネットセキュリティ組織であるCERT/CCの警告によって広く知られることになった。この警告は 2 年前に出されたが、産業技術総合研究所 高木 浩光 氏らの調査によると、8 割前後の web サイトがクロスサイト・スクリプティングに未対応であることが明らかになった。それによると、2001 年 10 月時点で多くの web サイトがこの脆弱性を抱えており、オンラインマークやプライバシーマークを取得している事業者の web サイトでさえも、対応しきれていない。（表）さらに、最近では、UFJ 銀行の web サーバにクロスサイト・スクリプティングの脆弱性が発見され、海外では、米 Yahoo、AOL、MSN などの大手 web サイトにもこの脆弱性があることが報告されている。インターネットの普及、それによる EC サイト等の増加により、潜在的にこのクロスサイト・スクリプティングの問題が存在する web サイトは多くあり、現在最も注目されている脆弱性の一つである。

表　クロスサイト・スクリプティングの問題を抱えているweb サイトの割合



プライバシーマーク---財団法人日本情報処理開発協会の定めるガイドラインに従って個人情報を適切に扱っていると認められた民間事業者が取得できる。

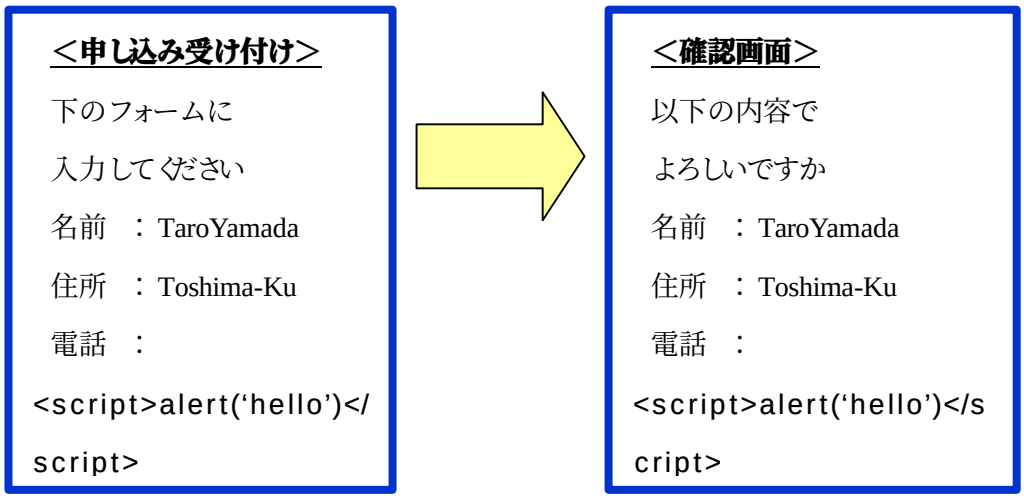
オンラインマーク---社団法人日本通信販売協会により、適切な消費者向け電子商取引を行っていると認められた民間事業者が取得できる。

(b) 仕組み

クロスサイト･スクリプティングの脆弱性は Cookie と密接に関係がある。Cookie とは主に会員制ウェブサイトなどで、ユーザとのセッションを管理するために、web サイトからユーザのブラウザに対し発行される小さなデータのことである。発行や読み取りには、JavaScript や CGI プログラムなどを用いる。web サイトは、Cookie の内容でどのユーザと通信中であるかを判断し、セッションを管理する。攻撃者はこの Cookie をクロスサイト･スクリプティングの脆弱性をついて盗むことにより、正規ユーザになりすまし、個人情報を取得することが可能になる。また、Cookie には有効期限があり、それを不適切に設定していると、一度盗まれてしまえば、永続的に盗用されてしまう。

クロスサイト･スクリプティングの脆弱性は、掲示板や情報検索サイト、登録情報の確認画面など、ユーザが入力した情報を元に、ウェブアプリケーションが動的に HTML ページを作成するようなウェブサイトにおいて発生する。ここでは、名前 ･住所 ･電話番号の三つの情報を入力するウェブサイトにおいて、入力した情報を、一度画面に表示して確認する機能が実装されている場合を例に挙げて説明する。

図　クロスサイト･スクリプティング脆弱性が存在しないサイトの場合

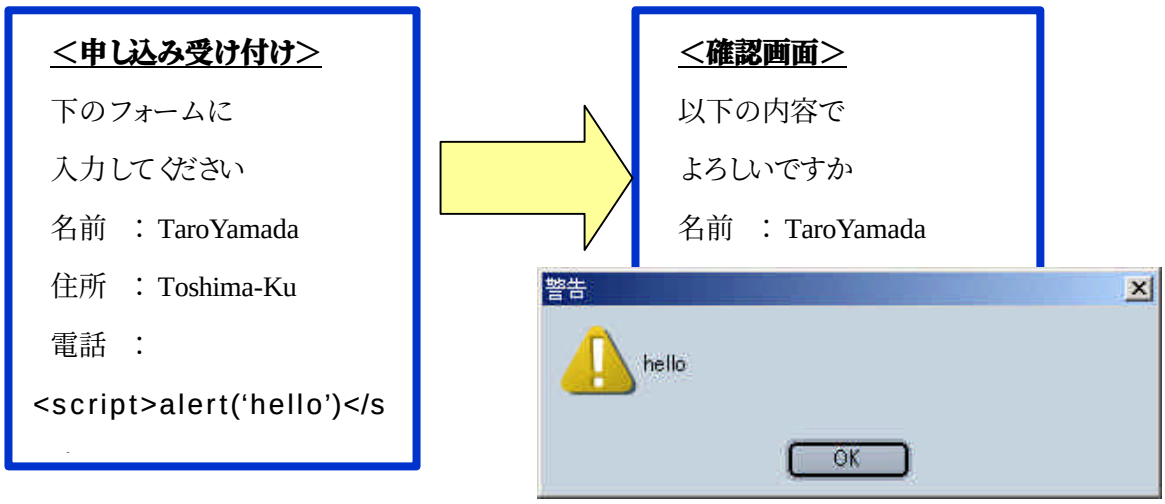


電話番号を入力する欄に、JavaScript を入力してしまったとしても、本来、単に入力情報を表示するのが目的の確認画面では、JavaScript の内容がそのまま表示されなければならな

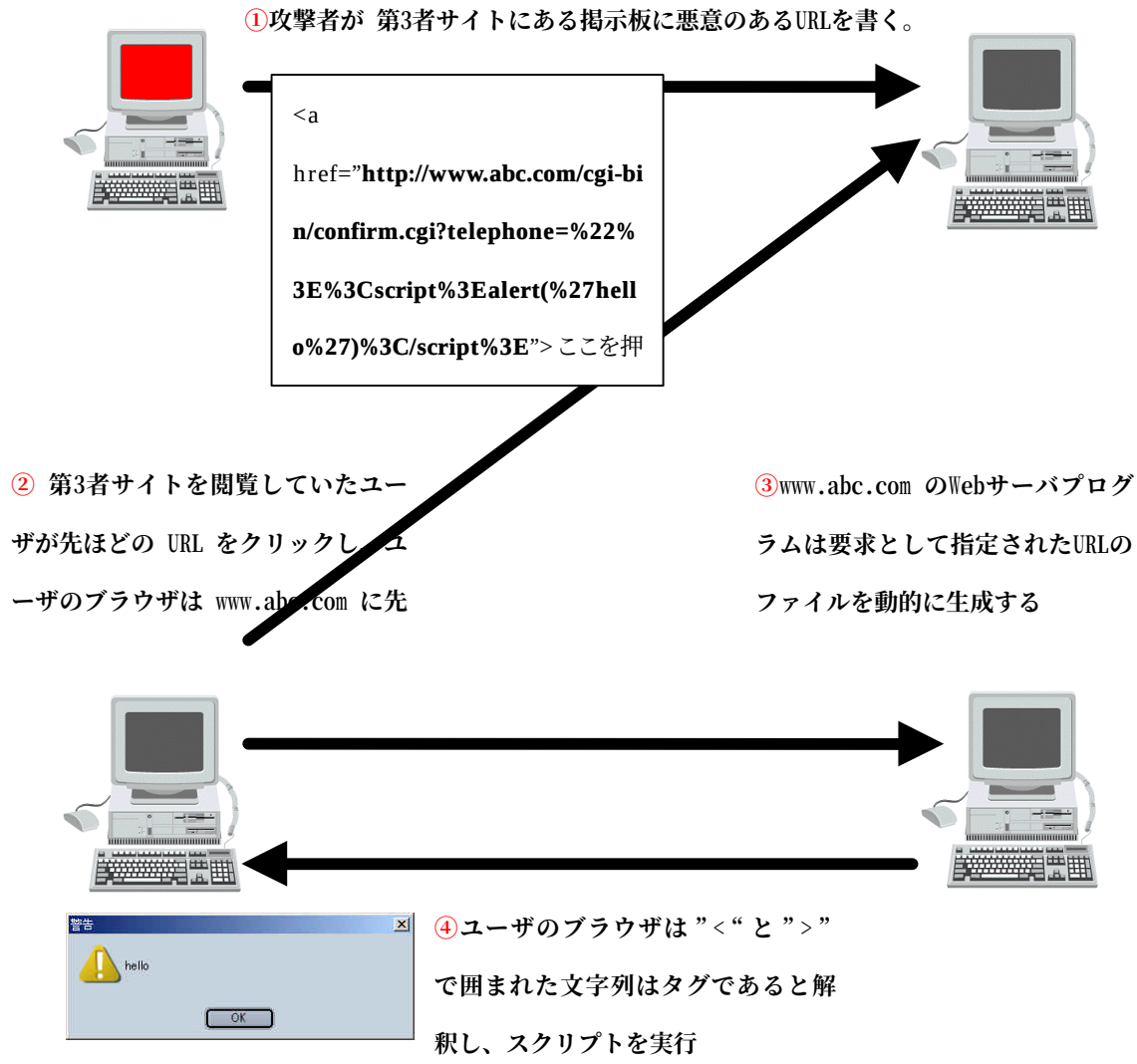
い。

しかし、クロスサイト・スクリプティング脆弱性が存在する web サイトでは、入力された JavaScript を解釈し、図 2 のように、確認画面において実行する。(この場合は警告ウィンドウを表示させる JavaScript が実行されている)。

図　クロスサイト・スクリプティング脆弱性が存在するサイトの場合



上記の例のような送信フォームの入力データは、多くの場合、CGI プログラムを利用している。例えば、これを利用して、無関係の第 3 者サイトに悪意のある攻撃者が以下のようなリンクを書き込んだとしたら、問題のあるサイト(この場合 www.abc.com)を経由して、ユーザのブラウザ上で JavaScript が実行されてしまう。



仮に悪意のある攻撃者が上記の JavaScript 部分に、ターゲットとなるユーザが www.abc.com 内で使用する Cookie を、攻撃者のサーバに送信するようなスクリプトを記述したとする。その www.abc.com へのリンクをクリックしたユーザはスクリプトを実行し、Cookie は読み取られ、攻撃者のサーバに送信されてしまう。このような手法により攻撃者はユーザの Cookie を盗み取ることが可能となる。

(c) 対策

① クライアント側での対策

クロスサイト・スクリプティングに対するクライアント側の対策としては、主として以下のようなものがあげられる。この脆弱性の問題は web サーバ側にあるため、クライアント側の対策

では本質的な解決に繋がらないが、有効な自衛策であることは確かである。

・疑わしいリンクへの警戒

攻撃者が「罠」として仕掛けたリンクを警戒することで、ある程度被害を防ぐことができる。

・会員制サイトへのログイン中は他サイトを閲覧せず、ログアウト後一度ブラウザを閉じる

発行される Cookie が一回のセッション限りのもので、ハードディスクには保存されない場合、ブラウザを閉ればメモリ上から Cookie を消すことが可能。

・ブラウザの設定で、JavaScript を無効、もしくは実行時に警告させる

JavaScript を無効にすることで、悪意のあるスクリプトを実行させない。

・ブラウザの設定で、Cookie の受け入れを無効、もしくは受け入れ時に警告させる

Cookie そのものの受け入れを制限することによって、Cookie の漏洩を防げる。

② web サーバ側での対策

web サーバ側で行うことができる対策として、以下のようなものがある。

・実行タグを解釈しないよう、web アプリケーションを開発

入出力データに実行タグ（スクリプト）が含まれても、解釈を行わないように設定する。

・クロスサイト・スクリプティングの脆弱性が存在しない web サーバを使用

web サーバの種類、バージョンによっては、web サーバ自身がこの脆弱性を持つ場合がある。多くの場合、新しいバージョンや修正プログラムが公開されているので、必要に応じて適用する。

・Cookie の乱用を避ける

セッション管理としての Cookie の利用を最小限にとどめることも有効な対策になる。使用する場合は、Cookie の有効期限を必要最小限にする。またその有効ドメインも必要最低限の範囲内にする。

第4章　付録

1. 参考資料

⑴ G8 におけるハイテク犯罪対策

(a) 欧米におけるコンピュータへの不正アクセス（クラッキング）と対策の実態調査

http://www.ipa.go.jp/security/fy11/report/contents/intrusion/jetro/creu99.html

(b) コンピュータ・ウィルス等有害プログラムの法的規制に関する国際動向調査（概要）

http://www.ipa.go.jp/security/fy11/report/contents/virus/law243.html

(c) ドイツにおけるコンピュータへの不正アクセス（クラッキング）とサイバーテロ対策の実態調査

http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/report_Germany.pdf

(d) 米国におけるコンピュータへの不正アクセス（クラッキング）とサイバーテロ対策の実態調査

http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/report_USA.pdf

(e) 国際的なハイテク犯罪（外務省）

http://www.mofa.go.jp/mofaj/gaiko/hitech/index.html

(f) G7／G8（外務省）

http://www.mofa.go.jp/mofaj/gaiko/summit/index.html

(g) 海外の関連法令

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/code/index.html

(h) 新世紀の法とコンピュータ（要約）

http://www.globetown.net/~ johotoho/c9inoue.htm

⑵ 韓国におけるハイテク犯罪対策

(a) 「インターネット犯罪の特徴と犯罪類型別の処罰条項」、韓国刑事政策研究院研究員、ウォンヘウク

(b) 「ハッキング犯罪とその処罰法規及び問題点」、韓国刑事政策研究院研究員、ベクカンフン

(c) 情報通信部　情報化政策関連　法令資料室

(d) 韓国侵害事故対応支援チーム

(e) 韓国情報保護振興院

(f) サイバー犯罪研究会

(g) 国家情報院

⑶ 中国におけるハイテク犯罪対策

(a) 『サイバークライシス』、宮脇磊介、PHP文庫

(b) 中国 IT 白書

http://it.searchina.ne.jp/

(c) 法情報学(夏井高人研究室)

http://www.isc.meiji.ac.jp/~ sumwel_h/

(d) 現代中国法ネットワーク

http://web.kyoto-inet.or.jp/people/chinalaw/index.html

(e) 日中法研究会

http://www2.justnet.ne.jp/~ zhangrong/link3.htm

(f) 中国でのインターネット規制

http://clinamen.ff.tku.ac.jp/CENSORSHIP/Overseas/China.html

(g) 中国ビジネス情報世界

http://www.jcbus.co.jp/reg/japan/

⑷ インドにおけるハイテク犯罪対策

(a) CICC (財)国際情報化協力センターシンガポール事務所 インドの IT 事情

http://www.cicc.org.sg/ciccrp/c3ir.html

(b) The information Technology Act, 2000 (概要)

http://www.winphatak.com/itact2000/index.htm

(c) Ministry of law, Justice And Company Affairs(Legislative Department) The Information Technology Act,2000 (原文)

http://www.mit.gov.in/itbill2000.pdf

(d) 社団法人 海外建設協会 シンガポールおよび周辺諸国の建設分野における IT の利用および普及状況

http://www.ocaji.or.jp/japanese/news/200104_3.html

(e) (財)日本情報処理開発協会 AITEC 先端技術研究所 先進諸国における将来の社会システムの情報化ビジョンに関する動向

http://www.icot.or.jp/FTS/REPORTS/H10-reports/AITEC9903Re1_Folder/AITEC9905R1-a6.html

(f) 日本機械輸出組合　インド電子商取引関連法制度の成立

http://www.jmcti.org/jmchomepage/jmcjournal/data/2000_11/bouekidoukou.pdf

(g) 日本政策投資銀行　インドの高等教育と人材育成

http://www.dbj.org.sg/PDF/S19j.pdf

⑸ マレーシアにおけるハイテク犯罪対策

(a) 「MSC Web Site」

http://www.mdc.com.my/msc/frame/policy.html

(b) 法情報学 夏井高人研究室）マレーシアのコンピュータ犯罪法

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/code/bill1997-a1.htm

(c) 「財団法人 国際通信経済研究所 第一研究部のご案内」、「マルチメディア・スーパー・コリドー計画とサイバー法 ―マレーシアの新たな挑戦―RITE97-J03S

http://www.rite-i.or.jp/rd1/reports/97J3S.htm

(d) 「ASEAN の通信放送法制 ―マレーシア―」RITE97-J03

http://www.rite-i.or.jp/rd1/reports/97J3.htm

(e) 「ASEAN の通信法制 ―マレーシアII ＜1998 年通信及びマルチメディアの関する法律＞―」RITE99-J03

http://www.rite-i.or.jp/rd1/reports/99J3.htm

(f) 「平成 11 年度 赤レンガ 政策検討プロジェクト 概要版」、資料１ 各国の情報通信産業関連政策

http://www.pref.hokkaido.jp/skikaku/sk-jkkku/akapuro/contents/report/lastgaiyou/gaiyouban.pdf

(g) COMPUTER CRIMES BILL 1997 英文

http://www.geocities.com/Tokyo/9239/comcrime.html

(h) 「Cyber Law, International Law and Asian Studies@wakhok」及び、「情報メディア入門 各国 IT 事情と政策－マレーシアを中心に」

http://www.wakhok.ac.jp/~ ichinohe/

http://www.wakhok.ac.jp/~ ichinohe/intro/20010711.ppt

(i) Malaysian Civil Service Link

http://mcsl.mampu.gov.my/

(j) 各国のサイバー法一覧

http://kjs.nagaokaut.ac.jp/mikami/EG/cyberlaw-list.htm

⑹ シンガポールにおけるハイテク犯罪対策

(a) アセアン諸国のインターネット普及率

http://web.kyoto-inet.or.jp/people/sisyphe/jpn/asean/asean4_it_04.htm

(b) シンガポールの IT 政策

http://www.ntt.com/sg/SINGAPORE/A30-03-00-00.html

http://www.cicc.org.sg/CiccNews/c3in079.html

http://www.csu.edu.au/special/conference/apwww95/papers95/jclark/jclark.html

(c) Computer Misuse Act

http://agcvldb4.agc.gov.sg/ (原文)

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/code/act1997-Singapore.htm

http://www.cnn.com/TECH/computing/9806/30/singapore.computing/

(d) 法律全般

http://www.ec.gov.sg/policy.html

http://home.talkcity.com/ChaplinCt/nhacvietmembers/singapore/IPR-Crime.html

(e) 事件

http://computertimes.asia1.com.sg/v20010829/issu08.shtml

http://www.it.mycareer.com.au/breaking/20000612/A61943-2000Jun12.html

(f) シンガポール IT の展望

http://asia.internet.com/asia-news/article/0,3916,161_661821,00.html

⑺ 欧州評議会におけるハイテク犯罪対策

(a) 欧州評議会「サイバー犯罪条約案（確定版）」（仮訳） 夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/cybercrimeconv-final.htm

(b) 欧州評議会「サイバー犯罪条約（確定版）

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

(c) 欧州評議会 『サイバー犯罪条約草案 (第 25 版)」(仮訳) 夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/cybercimeconv25.htm

(d) 欧州評議会 『サイバー犯罪条約草案 (第 25 版)」

http://www.cdt.org/international/cybercrime/001225cybercrime25.pdf

(e) 欧州評議会 『サイバー犯罪条約草案説明用覚書」(仮訳) 夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/expmemo25-1.htm

(f) サイバー犯罪条約 外務省仮訳

http://www.mainichi.co.jp/digital/zenbun/cyber-jouyaku/01.html

(g) Combating Economic and Organized crime, corruption, cybercrime, money laundering

http://www.legal.coe.int/economiccrime/Default.asp?fd=cybercrime&fn=PCCYMandatE.htm

(h) Recommendation (1989) 9 on computer-related crime

http://cm.coe.int/ta/rec/1989/89r9.htm

(i) Recommendation (1995) 13 concerning problems of criminal procedural law connected with information technology

http://cm.coe.int/ta/rec/1995/95r13.htm

(j) Frequently Asked Question and Answers About the Council of Europe convention on cyber crime

http://www.usdoj.gov/criminal/cybercrime/newCOEFAQs.html

(k) 583rd meeting of the Ministers ' Deputies, 4 February 1997 APPENDIX 13

http://cm.coe.int/dec/1997/583/583.a13.html

(l) 在ストラスブール日本国総領事館 「欧州評議会の概要」

http://mapage.noos.fr/consujap/ce.html#ce1

(m) JISA 第 5 回サイバー法セミナー資料 『サイバー犯罪条約と日本の刑事法制」夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/CyberCrimeTreatySeminar1.ppt

(n) JISA 第 6 回サイバー法セミナー資料 『サイバー犯罪条約を批准する場合の立法政策上の課題−手続法を中心に−」 夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/CyberCrimeTreatySeminar2d.ppt

(o) EU 加盟国閣僚理事会 情報技術と関係を有する刑事法手続き法規に関連する諸問題に関する勧告 NO.R (95) 13 (仮訳) 夏井高人

http://www.isc.meiji.ac.jp/~ sumwel_h/doc/intnl/recm_criminal_EU.htm

(p) アットマークIT Security & Trust 【特別企画】サイバー犯罪条約と国内法整備の課題

http://www.atmarkit.co.jp/fsecurity/special/14cyber/cyber01.html

(q) 欧州評議会 「サイバー犯罪条約」メモ 小倉利丸

http://www.jca.ax.apc.org/privacy/cyber_crime_intro.html

(r) 欧州評議会 法律問題に関するサイト －cyber crime－

http://www.legal.coe.int/economiccrime/Default.asp?fd=cybercrime&fn=IndexE.htm

(s) サイバー犯罪条約と警察権力のグローバル化

http://marux.org/~ ogura/cyber_crime_hihan.html

(t) ドイツにおけるコンピュータへの不正アクセス（クラッキング）とサイバーテロ対策の実態調査、情報処理振興事業協会

http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/report_Germany.pdf

(u) 米国におけるコンピュータへの不正アクセス（クラッキング）とサイバーテロ対策の実態調査 情報処理振興事業協会

http://www.ipa.go.jp/security/fy12/contents/crack/sekitoku/report_USA.pdf

(v) 日本経済新聞 2001 年 6 月 7 日記事 「サイバー犯罪条約の概要」

(w) 欧州評議会 サイバー犯罪条約報告書 社団法人 情報サービス産業協会

(8) 攻撃の傾向と手口

(a) CERT/CC 「CA-2000-02: Malicious HTML Tags Embedded in Client Requests」

http://www.cert.org/advisories/CA-2000-02.html (原文)

http://www.lac.co.jp/security/intelligence/CERT/CA-2000_02.html (邦訳)

(b) IPA 「Web サイトにおけるクロスサイト・スクリプティング脆弱性に関する情報」

http://www.ipa.go.jp/security/ciadr/20011023css.html

(c) 産業技術総合研究所 高木 浩光 氏ほか 「クロスサイト・スクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」

http://securit.etl.go.jp/research/paper/css2001-takagi-dist.pdf

(d) Microsoft 「クロスサイト スクリプティングのセキュリティ上の脆弱性に関する情報」

http://www.microsoft.com/JAPAN/technet/security/crssite.asp

(e) 株式会社ラック 最近のアタック」

http://www.lac.co.jp/security/news/attack/index.html

(f) 株式会社ラック　「SNSDB」

https://www.snsdb.com